7701/3701 Number Theory Notes

Based on the 2013 spring lectures by Dr R M Hill

MATH7701 – Number Theory

7 January 2013
Darwin LT
Dr Richard HILL.

Administrative Requirements:

- office hour Wed 10–11, Room 808
- Homework (10%). Distributed on Mondays, due Wednesday at Maths office
- Calculators (scientific standard) permitted in this course).

Overview of course.

Number theory is the theory of $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$ and similar rings. In this course, a ring is a set R with two operations $+$ and $\times$.

Rings are governed by the following axioms:

① $(R,+)$ is an abelian group with identity element 0.

② $\times$ is commutative with identity element 1.

③ Distributive action: $(a+b)\times c = ac + bc$.

e.g. $\mathbb{Z}$ is a ring, $\mathbb{Z}/n = \{0,1,\dots,n-1\}$ with addition and multiplication defined modulo n. $\mathbb{F}[x] = \{$polynomials with coefficients in field $\mathbb{F}\}$.

Chapters of the course are:

0) Review of material from other courses
1) Euler totient function, existence of primitive roots.
2) Quadratic reciprocity: is q a square mod p where p,q are prime?
3) Hensel's Lemma
4) Power series modulo p^n, where p is a prime number.
5) The Gaussian integers $\mathbb{Z}[i] = \{x+iy : x,y \in \mathbb{Z}\}$
6) Continued fractions and Pell's equation, $x^2 - dy^2 = 1$.

Section 0
PREVIOUSLY-SEEN MATERIAL.

Let n be a positive integer. Then $x,y \in \mathbb{Z}$ are congruent mod n if $x-y$ is a multiple of n. This is denoted $x \equiv y \pmod n$ or $x \equiv y\ (n)$.

We also write $\mathbb{Z}/n$ for the integers modulo n, i.e. the usual integers but where x and y are regarded as the same if $x \equiv y \pmod n$.

Solving linear congruences.

Consider the system $ax \equiv b \pmod n$ given a,b,n.

Case 1: Suppose a is invertible mod n; equivalently a,n are coprime. i.e. $\exists\, a^{-1} \in \mathbb{Z}/n$ with $a\cdot a^{-1} \equiv 1 \bmod n$.

In this case, we solve by multiplying both sides by a^{-1}, which can be found by reverse Euclidean algorithm. Then $a^{-1}\cdot ax \equiv a^{-1}b \bmod n \Rightarrow x \equiv a^{-1}b \bmod n$.

Case 2: Suppose n is a multiple of a. In this case, we get the solution to $ax \equiv b \bmod n$ as follows:

- If b is not a multiple of a, there are no solutions.
- If b is also a multiple of a, then $x \equiv \frac{b}{a} \pmod{\frac{n}{a}}$

$\boxed{\text{Ex}}$ Solve $5x \equiv 11 \bmod 13$.

Soln. $5,13$ are coprime $\Rightarrow$ Find 5^{-1} in $\mathbb{Z}_{13}$. $13 = 2\cdot5+3$, $5 = 1\cdot3+2$, $3 = 1\cdot2+1 \Rightarrow 1 = 1\cdot3 - 1\cdot2 = 1\cdot3 - 1\cdot(1\cdot5 - 1\cdot3) = 2\cdot3 - 1\cdot5 = 2\cdot(1\cdot13 - 2\cdot5) - 1\cdot5 = 2\cdot13 - 5\cdot5$

Take mod 13, $-5\cdot5 \equiv 1$ so $5^{-1} \equiv -5 \equiv 8 \bmod 13$. Hence, $5x \equiv 11 \Rightarrow x \equiv 8\cdot11 \pmod{13} \equiv 88 \equiv 10 \pmod{13}$. $x = 13n+10$ //

$\boxed{\text{Ex}}$ Solve $7x \equiv 84 \bmod 490$.

Soln. $7|490$. Since $7|84$ as well, a solution exists. Then $x \equiv 12 \bmod 70$. $\Rightarrow x = 70n+12$ //.

$\boxed{\text{Ex}}$ Solve $7x \equiv 85 \bmod 490$.

Soln. $7|490$. However, $7\nmid 85 \Rightarrow$ no solution //

$\boxed{\text{Ex}}$ Solve $6x \equiv 3 \bmod 21$.

Soln. $6,21$ are not coprime. Neither case 1 or 2. Then we write $3(2x) \equiv 3 \bmod 21$. Apply case 2, since $3|21$, $3|3$. Then $2x \equiv \frac{3}{3} \bmod \frac{21}{3}$.

We get $2x \equiv 1 \bmod 7$. By inspection, $2^{-1} = 4 \bmod 7$ s.t. $x \equiv 4 \bmod 7$, $x = 7n+4$ //.

8 January 2012
Darwin LT
Dr Richard HILL

Chinese Remainder Theorem.

Suppose we have an integer x and we know $x \bmod 10$, then we know $x \bmod 5$ and $x \bmod 2$. e.g. if $x \equiv 7 \bmod 10$, $x \equiv 2 \bmod 5$, $1 \bmod 2$.

The Chinese Remainder theorem allows us to go the other way.

$\boxed{\text{Theorem}}$ (Chinese Remainder theorem)

Suppose n, m coprime, and $a \in \mathbb{Z}/n$ and $b \in \mathbb{Z}/m$, then $\exists$ unique $x \in \mathbb{Z}/nm$ s.t. $x \equiv a \pmod n$ and $x \equiv b \pmod m$

Proof – (only the existence part; for proof of uniqueness see MATH1202.)

Since n, m are coprime, $\exists\, h, k \in \mathbb{Z}$ s.t. $hn + km = 1$. $\therefore hn \equiv 1 \pmod m$, $km \equiv 1 \pmod n$. Obviously, $hn \equiv 0 \pmod n$, $km \equiv 0 \pmod m$

Let $x \equiv hnb + kma \bmod mn$. Then x is a solution to these equations, as $x \equiv kma \equiv a \pmod n$, $x \equiv hnb \equiv b \pmod m$// q.e.d.

$\boxed{\text{Ex}}$ Solve $x \equiv 3 \pmod 8$ and $x \equiv 4 \pmod 5$.

Soln. Note that $\gcd(8,5) = 1$, so we can apply CRT. $8 = 1\cdot5+3$, $5 = 1\cdot3+2$, $3 = 1\cdot2+1 \Rightarrow 1 = 1\cdot3 - 1\cdot2 = 2\cdot3 - 1\cdot5 = 2\cdot(1\cdot8 - 1\cdot5) - 1\cdot5 = 2\cdot8 - 3\cdot5$.

Then $x \equiv 4\cdot2\cdot8 - 3\cdot3\cdot5 \equiv 64 - 45 \equiv 19 \pmod{40}$//

We can also use the Chinese Remainder theorem to solve more complicated congruences modulo nm (where $\text{hcf}(n,m) = 1$).

We solve mod m and mod n, then put solutions together using CRT.

$\boxed{\text{Ex}}$ Solve $x^2 \equiv 2 \pmod{119}$

Soln. Use property that 119 factorises into two coprime factors, $119 = 7 \times 17$. Then $x^2 \equiv 2 \pmod 7$, $x^2 \equiv 2 \pmod{17}$.

$x^2 \equiv 2 \equiv 9 \pmod 7 \Rightarrow x \equiv \pm 3 \bmod 7$. $x^2 \equiv 2 \equiv 36 \pmod{17} \Rightarrow x = \pm 6 \bmod 17$. Perform Euclid's algorithm with 7 and 17:

$17 = 2\cdot7+3$, $7 = 2\cdot3+1 \Rightarrow 1 = 1\cdot7 - 2\cdot3 = 1\cdot7 - 2(1\cdot17 - 2\cdot7) = 5\cdot7 - 2\cdot17$. $x \equiv 5\cdot7\cdot(\pm6) - 2\cdot17(\pm3) \equiv \pm210 \mp 102 \equiv \pm210 \pm 102 \pmod{119}$

We have 4 solutions: $x \equiv \pm210 \pm 102 \equiv \pm28 \pm 17 \equiv \pm11$ or $\pm45 \equiv 11, 45, 74, 108 \pmod{119}$//

Fermat's Little theorem.

A prime number is an integer $p \geq 2$ s.t. its factors are $\pm1, \pm p$ only. We write $\mathbb{F}_p$ instead of $\mathbb{Z}/p$ to denote the set of integers modulo p. This is because $\mathbb{F}_p$ is a field.

$\boxed{\text{Theorem}}$ $\mathbb{Z}/p$ (or $\mathbb{F}_p$) is a field.

Proof – (sketch): $1, 2, \dots, p-1$ are coprime to p. Thus, $\exists\, h, k \in \mathbb{Z}$ s.t. $1 = hp + kr$ for $r \in \mathbb{Z}/p \Rightarrow \exists\, k \in \mathbb{Z}$ s.t. $kr \equiv 1 \pmod p \Rightarrow$

every element in $\mathbb{Z}/p$ except 0 has an inverse $\Rightarrow \mathbb{Z}/p$ is a field// q.e.d.

$\boxed{\text{Corollary}}$ (Fermat's little theorem)

Let $a \in \mathbb{F}_p^\times$ (i.e. $a \in \mathbb{F}_p$ and $a \not\equiv 0 \pmod p$). Then $a^{p-1} \equiv 1 \pmod p$.

Proof – $\mathbb{F}_p^\times = \{1, 2, 3, \dots, p-1\}$ is a group with the operation multiplication. The group has $p-1$ elements. Let n be the order of a in $\mathbb{F}_p^\times$.

By Lagrange's theorem, $n = o(a) \mid p-1$ i.e. $p-1 = nm$ for some $m \in \mathbb{Z}$. Then $a^{p-1} \equiv a^{nm} \equiv a^{o(a)m} \equiv 1^m \equiv 1 \bmod p$// q.e.d.

We can use Fermat's little theorem to solve congruences of the form $x^a \equiv b \ (p)$ where p is prime; a is coprime to $p-1$ (i.e. a is invertible mod $p-1$).

To do this, find the inverse of a mod $p-1$. Call this c, i.e. $ac = 1 + (p-1)r$ for some $r \in \mathbb{Z}$. Raise both sides of the equation to power c.

$x^a \equiv b \bmod p \Rightarrow x^{ac} \equiv b^c \bmod p \Rightarrow x^{1+(p-1)r} \equiv x(x^{p-1})^r \equiv x(1)^r \equiv x \equiv b^c \bmod p$. We solve from here.

$\boxed{\text{Ex}}$ Solve $x^5 \equiv 2 \pmod{19}$.

Soln. Checking, we note that 19 is prime, and $\gcd(5, 19-1) = \gcd(5, 18) = 1$. We seek $5^{-1} \bmod 18$. $18 \equiv 3\cdot5+3$, $1\cdot5 = 1\cdot3+2$, $3 = 1\cdot2+1$; so

$1 \equiv 2\cdot3 - 1\cdot5 \equiv 2(1\cdot18 - 3\cdot5) - 1\cdot5 \equiv 2\cdot18 - 7\cdot5$, so $5^{-1} \equiv -7 \bmod 18 \equiv 11$. $x^5 \equiv 2 \pmod{19} \Rightarrow x^{55} \equiv 2^{11} \pmod{19} \Rightarrow x \equiv 2048 \bmod 19 \equiv 148 \equiv 15$//

14 January 2013
Dr. Richard Hill
Darwin LT.

$\boxed{\text{Theorem}}$ (Fundamental theorem of Arithmetic)

Let n be a positive integer, then there is a unique factorisation $n = p_1 p_2 \cdots p_r$; ($p_1, \dots, p_r$ are prime), up to rearrangement

Proof – see MATH1201.

$\boxed{\text{Theorem}}$ There are infinitely many primes.

Proof – Suppose $p_1, \dots, p_r$ are all the prime numbers. Let $N = p_1 p_2 \cdots p_r + 1 \Rightarrow N$ is not a multiple of $p_1, \dots, p_r$. Also $N > 1$, so N is prime

$\therefore$ there are more than n prime numbers $\Rightarrow$ infinitely many primes// q.e.d.

Sieve of Eratosthenes:

If n is a composite number, $n > 1$, then n has a prime factor $p \leq \sqrt{n}$. We can check whether a number is prime or not, using this:

$\boxed{\text{Ex}}$ Determine if 199 is prime:

Soln. $14 < \sqrt{199} < 15$. So we just need to check whether 199 is a multiple of a prime $p < 15$. The primes < 15 are $2, 3, 5, 7, 11, 13$.

Checking all these potential divisors, none divide 199 $\Rightarrow$ 199 is prime.

Chapter 1

EULER TOTIENT FUNCTION.

Recall that $(\mathbb{Z}/n)^\times$ refers to the set of $x \in \mathbb{Z}/n$ which are invertible mod n. i.e. $\{x \in \mathbb{Z}/n \mid \exists y \in \mathbb{Z}/n \text{ st. } xy \equiv 1 \bmod n\}$.

$(\mathbb{Z}/n)^\times$ is a group with the operation $\times$.

e.g. $(\mathbb{Z}/4)^\times = \{1,3\}$, with multiplication table

×	1	3
1	1	3
3	3	1

; $(\mathbb{Z}/6)^\times = \{1,5\}$,

×	1	5
1	1	5
5	5	1

; $(\mathbb{Z}/8)^\times = \{1,3,5,7\}$,

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

.

$\boxed{\text{Definition}}$ The Euler totient function is defined by $\varphi(n) = |(\mathbb{Z}/n)^\times|$.

e.g. $\varphi(4)=2$, $\varphi(6)=2$, $\varphi(8)=4$.

$\boxed{\text{Proposition}}$ If p is a prime, $\varphi(p) = p-1$.

Proof – p is prime $\Rightarrow$ $\mathbb{Z}/p = \mathbb{F}_p$ is a field. $\Rightarrow \varphi(p) = p-1$ // q.e.d.

$\boxed{\text{Theorem}}$ (Euler's Theorem)

If $x \in (\mathbb{Z}/n)^\times$, then $x^{\varphi(n)} \equiv 1 \pmod n$.

Remark: If $n=p$ is prime, we get Fermat's little theorem.

Proof – $x \in (\mathbb{Z}/n)^\times$, which is a group that has $\varphi(n)$ elements. Let $r = \operatorname{ord}(x)$, so $x^r \equiv 1\ (n)$. By Lagrange's Theorem, $r = \operatorname{ord}(x) \mid \varphi(n)$.

Thus, $x^{\varphi(n)} \equiv x^{kr} \equiv (x^r)^k \equiv 1^k \equiv 1 \pmod n$.

In order to use this, we require a quick way of calculating $\varphi(n)$.

$\boxed{\text{Lemma}}$ Let $n = p^a$ where p is prime and $a \in \mathbb{N}$. Then $\varphi(n) = (p-1)p^{a-1}$.

e.g. $\varphi(8) = \varphi(2^3) = (2-1)\cdot 2^{3-1} = 1\cdot 2^2 = 4$, $\varphi(9) = \varphi(3^2) = (3-1)\cdot 3^{2-1} = 2\cdot 3 = 6$.

Proof – If $x \in \mathbb{Z}/p^a$, then x is not invertible mod p^a $\Leftrightarrow$ $\operatorname{hcf}(x,p^a) > 1$. But this $\operatorname{hcf}(x,p^a)$ is a factor of p^a $\Rightarrow$ $\operatorname{hcf}(x,p^a) = p$ or p^2 or $\cdots$ or p^a.

Thus, $p \mid x$. Conversely, if $p \mid x$, then $\operatorname{hcf}(x,p^a) > 1$ $\Rightarrow$ the multiples of p are the numbers which are not invertible mod p^a.

$\therefore$ the elements of $\mathbb{Z}/p^a$ without inverses are $a, p, 2p, \cdots, p^a - p$. There are p^{a-1} of these. $\therefore |(\mathbb{Z}/p^a)^\times| = p^a - p^{a-1} = (p-1)p^{a-1}$ // q.e.d.

$\boxed{\text{Theorem}}$ Suppose n,m are coprime, then $(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$. [Recall: If G,H are groups, then $G \times H = \{(g,h) : g \in G, h \in H\}$ is a group].

$\boxed{\text{Corollary}}$ If n,m are coprime, $\varphi(nm) = \varphi(n)\varphi(m)$.

Proof – $\varphi(nm) = |(\mathbb{Z}/nm)^\times| = |(\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times| = |(\mathbb{Z}/n)^\times||(\mathbb{Z}/m)^\times| = \varphi(n)\varphi(m)$ // q.e.d.

Remark: Given any integer $n>0$, $n = p_1^{d_1} \cdots p_r^{d_r}$, where $p_1, \cdots, p_r$ are distinct primes. By corollary, $\phi(n) = \phi(p_1^{d_1}) \cdots \phi(p_r^{d_r}) = \prod_{i=1}^{r} (p_i - 1)p^{d_i - 1}$.

Using this formula, we can technically calculate many values of $\varphi(n)$. Define $\varphi(1)=1$, then e.g.

$\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=\varphi(2)\varphi(3)=1\cdot 2=2$, $\varphi(7)=6$, $\varphi(8)=\varphi(2^3)=4$, $\varphi(9)=\varphi(3^2)=6$, $\varphi(10)=\varphi(2)\varphi(5)=4$.

$\varphi(300) = \varphi(4)\varphi(3)\varphi(25) = \varphi(3)\varphi(2^2)\varphi(5^2) = 2\cdot(1\cdot 2^1)\cdot(4\cdot 5^1) = 80$.

e.g. $(\mathbb{Z}/20)^\times \cong (\mathbb{Z}/4)^\times \times (\mathbb{Z}/5)^\times$, so $(\mathbb{Z}/4)^\times \times (\mathbb{Z}/5)^\times = \{(1,1), (1,2), (1,3), (1,4), (3,1), (3,2), (3,3), (3,4)\}$. $f(n) = (n \bmod 4, n \bmod 5)$ is a bijection.

Proof – We define a function $\Phi : \mathbb{Z}/nm \cong \mathbb{Z}_n \times \mathbb{Z}_m$, n,m coprime. By Chinese Remainder theorem, Φ is a bijection.

$\Phi(xy) = (xy \bmod n, xy \bmod m) = (x \bmod n, x \bmod m)\cdot(y \bmod n, y \bmod n) = \Phi(x)\Phi(y)$. So, it remains to check that $\Phi((\mathbb{Z}/nm)^\times) = (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$.

This is equivalent to showing that x is invertible mod nm $\Leftrightarrow$ x is invertible mod m and mod n. Suppose x is invertible mod nm.

Let $y = x^{-1} \bmod nm$, $xy \equiv 1\ (nm)$ $\Rightarrow$ $xy = knm + 1$ $\Rightarrow$ $xy \equiv 1\ (n)$, $xy \equiv 1\ (m)$ $\Rightarrow$ x is invertible mod m and mod n. Conversely,

assume x is invertible mod n, and also mod m. Let $a \equiv x^{-1}\ (n)$, $b \equiv x^{-1}\ (m)$. Then $xa \equiv 1\ (n)$, $xb \equiv 1\ (m)$

By the Chinese Remainder Theorem, $\exists y \in \mathbb{Z}$ s.t. $y \equiv a\ (n)$, $y \equiv b\ (m)$ $\Rightarrow$ $xy \equiv xa \equiv 1\ (n)$, $xy \equiv xb \equiv 1\ (m)$. By the uniqueness criterion of the Chinese Remainder Theorem, y is a unique solution to $xy \equiv 1\ (nm)$ $\Rightarrow$ x is invertible mod nm // q.e.d.

Recall that we have a formula for $\varphi(n)$: If $n = p_1^{a_1} \cdots p_r^{a_r}$, then $\varphi(n) = (p_1 - 1)p_1^{a_1 - 1} \cdots (p_r - 1)p_r^{a_r - 1}$.

We now use this to solve congruences modulo n in the same way that we used Fermat's little theorem for prime n.

Solving: $x^a \equiv b \pmod n$, given that b,n are coprime and $a, \varphi(n)$ are coprime.

Method –
- Factorise n and calculate $\varphi(n)$
- Find a^{-1} modulo $\varphi(n)$. Raise both sides of equation to power a^{-1}. Then

$x^{aa^{-1}} \equiv b^{a^{-1}} \bmod n \Rightarrow x \equiv b^{a^{-1}} \bmod n$.

$\boxed{\text{Ex}}$ Solve $x^7 \equiv 3 \bmod 50$.

Soln. $50 = 2 \times 5^2$, $\varphi(50) = 1 \times (4 \cdot 5) = 20$. $\gcd(7,20) = 1$ and $\gcd(3,50) = 1$. $20 = 2\cdot 7 + 6 \Rightarrow 1 = 1\cdot 7 - 1\cdot 6 = 1\cdot 7 - 1\cdot(1\cdot 20 - 2\cdot 7) = 3\cdot 7 - 1\cdot 20$

$7^{-1} \equiv 3 \bmod 20$. Then $(x^7)^3 \equiv 3^3 \Rightarrow x \equiv 27 \bmod 50$ //.

Remark: We can actually use negative remainders with Euclid's algorithm: $20 = 3\cdot 7 - 1 \Rightarrow 1\cdot 20 - 3\cdot 7 = -1 \Rightarrow 3\cdot 7 - 1\cdot 20 = 1$

15 January 2013
Dr. Richard HILL
Darvin LT

<u>Primitive Roots</u>.

A group G is cyclic if $\exists g \in G$ s.t. every element is of form g^n for some integer n. The element g is called a generator of g.

Equivalently, if G is a finite group, $\mathrm{ord}(g) = |G|$.

Standard examples: $\mathbb{Z}/n$ with the operation of addition. 1 is a generator (every element is a multiple of 1).

$\boxed{\text{Theorem}}$ (Gauss) For any prime p, $\mathbb{F}_p^\times$ is cyclic.

$\boxed{\text{Definition}}$ A <u>primitive root</u> modulo p is a generator for $\mathbb{F}_p^\times$, or equivalently an element of order $p-1$.

e.g. If $p = 7$, 1 is not a primitive root. Try 2: $2^2 = 4$, $2^3 = 8 \equiv 1 \Rightarrow \mathrm{ord}(2) = 3$. Try 3: $3^1 = 3$, $3^2 = 9 \equiv 2$, $3^3 = 3^2\cdot 3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1 \bmod 7$.

$\mathrm{ord}(3) = 6 \Rightarrow 3$ is a primitive root mod 7. $\mathbb{F}_7^\times = \{1, 3, 2, 6, 4, 5\}$

$\boxed{\text{Proposition}}$ Let p be a prime and $a \in \mathbb{F}_p^\times$. Then a is a primitive root modulo $p \iff \forall$ prime factors $q \mid p-1$, $a^{\frac{p-1}{q}} \not\equiv 1 \bmod p$.

Proof – Assume $a^{\frac{p-1}{q}} \equiv 1$ for some prime $q \mid p-1$. Then $\mathrm{ord}(a) < p-1$. So a is not a primitive root. Conversely, assume a is not a primitive root, i.e. $\mathrm{ord}(a) = d < p-1$. By Lagrange's theorem, $d \mid p-1$, $d < p-1$. Then $\frac{p-1}{d} \in \mathbb{Z}$. Let q be a prime factor of $\frac{p-1}{d}$.

i.e. $\frac{p-1}{d} = qm$ for some $m \in \mathbb{Z}$. $a^{\frac{p-1}{q}} = a^{dm} \Rightarrow a^{\frac{p-1}{q}} = (a^d)^m \equiv 1^m \equiv 1 \bmod p$. Take contrapositives // q.e.d.

We will use this to find the primitive roots modulo 29: $p = 29$, $p-1 = 28$. Then $28 = 2^2 \times 7$; $2, 7 \mid 28 \Rightarrow$ prime factors, q, of 28 are just 2 and 7.

$\therefore$ a is a primitive root mod $29 \iff a^{28/2} \not\equiv 1 \bmod 29$ and $a^{28/7} \not\equiv 1 \bmod 29$. Try $a = 2$. $2^4 \equiv 16 \not\equiv 1 \bmod 29$, $2^{14} \equiv 2^5\cdot 2^5\cdot 2^4 \equiv (32)^2\cdot 16 \equiv 3^2\cdot 16 \equiv 28 \not\equiv 1$

$\Rightarrow 2$ is a primitive root, modulo 29. 3 is also a primitive root mod 29......

It remains to show that $\mathbb{F}_p^\times$ is cyclic i.e. primitive roots exist, modulo p prime (Gauss's Theorem).

$\boxed{\text{Lemma}}$ An element $x \in \mathbb{Z}/n$ (additive group) is a generator is a generator of $\mathbb{Z}/n \iff x \in (\mathbb{Z}/n)^\times$.

i.e. $\varphi(n) = |(\mathbb{Z}/n)^\times|$ gives the number of generators of a cyclic group of order n.

Proof – ($\Leftarrow$): Assume $x \in (\mathbb{Z}/n)^\times$. Then it is invertible under $\times$, some multiple of x is 1 in $\mathbb{Z}/n$. $\therefore$ every element of $\mathbb{Z}/n$ is a multiple of x.

$\Rightarrow x$ generates $\mathbb{Z}/n$.

($\Rightarrow$): Conversely if x generates $\mathbb{Z}/n$, then every element of $\mathbb{Z}/n$ is a multiple of x. In particular, 1 is a multiple of x $\therefore x \in (\mathbb{Z}/n)^\times$.

$\boxed{\text{Lemma}}$ Let $d \mid n$. Then $\exists$ unique subgroup of $\mathbb{Z}/n$ with d elements. This subgroup is $\{0, \frac{n}{d}, \frac{2n}{d}, \dots, \frac{(d-1)n}{d}\}$.

$\varphi(d)$ gives the number of elements of order d in $\mathbb{Z}/n$.

Proof – Clearly, $\{0, \frac{n}{d}, \dots, \frac{(d-1)n}{d}\}$ is a subgroup with d elements. Let $H = \{0, \frac{n}{d}, \dots, \frac{(d-1)n}{d}\}$. Let H' be another subgroup of d elements.

Let $x \in H'$. Then $\mathrm{ord}(x) \mid d \Rightarrow dx \equiv 0 \pmod n$. $\Rightarrow x \equiv 0 \bmod \frac{n}{d}$. Thus x is a multiple of $\frac{n}{d} \Rightarrow x \in H \Rightarrow H' \subset H$, but

$|H| = |H'| = d$, so $H = H' \Rightarrow H$ is unique. // q.e.d. Now suppose x is an element of order d.

$\therefore$ subgroup generated by x has d elements $\therefore$ this subgroup is H. $\therefore x \in H$. $\Rightarrow \left|\begin{smallmatrix}\text{elements of}\\ \text{order } d \text{ in } \mathbb{Z}/n\end{smallmatrix}\right| = \left|\begin{smallmatrix}\text{elements of}\\ \text{order } d \text{ in } H\end{smallmatrix}\right|$. But H is cyclic

of order d, so $H \cong \mathbb{Z}/d$. By the previous lemma, $\exists\ \varphi(d)$ elements of order d.

$\boxed{\text{Proposition}}$ For any positive integer n, $\sum_{d \mid n} \varphi(d) = n$. (sum over all factors of n).

e.g. $n = 6$, $6 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + \varphi(2)\varphi(3) = 1 + 1 + 2 + 2 = 6$.

Proof – Every element of $\mathbb{Z}/n$ has order d for some $d \mid n$. There are exactly $\varphi(d)$ elements of order d. $\therefore n = \sum_{d \mid n} \varphi(d)$.

21 January 2013
Dr. Richard HILL
Darvin LT.

$\boxed{\text{Theorem}}$ Let p be any prime, then $\exists$ a primitive root modulo p. In fact, there are $\varphi(p-1)$ of them.

The proof will require some other results:

- the number of elements of order d in the additive group $\mathbb{Z}/d$ is $\varphi(d)$.
- If $d \mid n$, then # elements of order d in $\mathbb{Z}/n$ is $\varphi(d)$
- $\sum_{d \mid n} \varphi(d) = n$

We also recall a result from MATH2201:

- Let $\mathbb{F}$ be any field, and $f(x) \in \mathbb{F}[x]$. Then f has at most d zeros in $\mathbb{F}$, where $d = \deg(f)$.

(Theorem)
Proof – Let $d|p-1$, define $H=\{x \in \mathbb{F}_p^\times : x^d \equiv 1 \bmod p\}$. We note that ① H is a subgroup of $\mathbb{F}_p^\times$. If $x,y \in H$, then $x^d \equiv y^d \equiv 1\ (p)$ $\therefore (xy)^d \equiv x^d y^d \equiv 1\ (p)$.

② $|H| \le d$, as any element of H is a root of the polynomial $x^d - 1$. ③ If $x \in \mathbb{F}_p^\times$ has order d, then $x \in H$ (obviously). Then H is a cyclic gp of order d, generator x.

Let $N(d)$ = number of elements of order d in $\mathbb{F}_p^\times$. Then by ③, $N(d)$ = # elements of order d in H = $\begin{cases} \varphi(d) & \text{if } H \text{ is cyclic of order } d \\ 0 & \text{by ③.} \end{cases}$

Certainly, $N(d) \le \varphi(d)$. Then $\sum_{d|p-1} N(d) = |\mathbb{F}_p^\times| = p-1$. Also, $\sum_{d|p-1} \varphi(d) = p-1$ by proposition and for any d, $N(d) \le \varphi(d)$.

$\therefore N(d) = \varphi(d)\ \forall\, d|p-1$. In particular, $\exists\ \varphi(p-1)$ elements of order $p-1$.// q.e.d.

chapter 2

QUADRATIC RECIPROCITY.

This is about quadratic equations modulo a prime number p. Recall thus far, to solve $x^a \equiv b \bmod p$, we need a to be invertible mod $p-1$.

If $p \ge 3$, $p-1$ is even, and method will not work for $a=2$.

We will not actually solve quadratic equations modulo p. Instead, we will just find out whether it has solutions.

Definition Let p be an odd prime (i.e. $p \ge 3$) and let $a \in \mathbb{F}_p^\times$. Then a is a <u>quadratic residue modulo p</u> if $a \equiv x^2$ for some $x \in \mathbb{F}_p^\times$.

Otherwise, we call a a <u>quadratic non-residue modulo p</u>.

We define the quadratic residue symbol $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \\ -1 & \text{if } a \text{ is a quadratic non-residue.} \end{cases}$ [defined only if a,p are coprime]

Ex Calculate $\left(\frac{i}{5}\right)$ for $i \in \mathbb{F}_5^\times$.

Soln. We have:

x	1	2	3	4
x^2 mod 5	1	4	4	1

$\Rightarrow \left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = +1$// , $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$// .

Theorem (Euler's Criterion)

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Proof – By Fermat's little theorem, RHS squared is $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \bmod p$. $\therefore a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.

Suppose a is a quadratic residue, i.e. $a = x^2 \bmod p$; then $a^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \bmod p$.

Now suppose a is a quadratic non-residue instead. Let g be a primitive root modulo p. Then $a = g^r$ for some r. r is odd, since r even $\Rightarrow a$ is a square.

$a^{\frac{p-1}{2}} \equiv g^{\frac{(p-1)r}{2}} \equiv (g^{p-1})^{\frac{r}{2}}$. Since r is odd, $\frac{r}{2} \notin \mathbb{Z}$ so $\frac{(p-1)r}{2}$ is not a multiple of $p-1$, but $\text{ord}(g) = p-1 \Rightarrow g^{\frac{(p-1)r}{2}} \not\equiv 1 \bmod p \Rightarrow a^{\frac{p-1}{2}} \not\equiv 1 \bmod p$// q.e.d.

Ex Calculate $\left(\frac{a}{7}\right)$ using Euler's Criterion.

Soln.

a	1	2	3	4	5	6
$\left(\frac{a}{7}\right)$	1	1	-1	1	-1	-1

// . By Euler's criterion, $\left(\frac{a}{7}\right) \equiv a^3 \bmod 7 \Rightarrow 1,2,4$ are quadratic residues (squares mod 7)

Corollary $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof – $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$// q.e.d.

Corollary The set of quadratic residues mod p is a subgroup of index 2 in $\mathbb{F}_p^\times$, i.e. $\exists\ \frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ non-residues.

Proof – By previous corollary, the map $\mathbb{F}_p^\times \to \{1,-1\}$ is a group homomorphism. Then quadratic residues form the kernel of this map.

We just need to show this map is surjective. Let g be a primitive root modulo p. Then $\text{ord}(g) = p-1 \Rightarrow g^{\frac{p-1}{2}} \not\equiv 1 \bmod p \Rightarrow \left(\frac{g}{p}\right) \equiv -1 \bmod p$.

By Euler's criterion, $\left(\frac{g}{p}\right) \equiv -1$// q.e.d.

<u>Quadratic Reciprocity Law</u>

Suppose we have two distinct odd primes p and q. We can calculate $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$.

Theorem For distinct odd primes p and q, $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$.

Proof will be provided later. Note that $(-1)^{\frac{(p-1)(q-1)}{4}}$ is $+1$ if $p \equiv 1\ (4)$ or $q \equiv 1\ (4)$; is -1 if $p \equiv q \equiv -1\ (4)$.

Theorem If p is an odd prime, then (i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, and (ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \bmod p$. $\leftarrow \begin{cases} 1 & \text{if } p \equiv \pm 1\ (8) \\ -1 & \text{if } p \equiv \pm 3\ (8) \end{cases}$

Proof – (i) $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$ by Euler's criterion// q.e.d

(ii)

These theorems allow us to calculate $\left(\frac{a}{p}\right)$ very quickly.

Ex Calculate $\left(\frac{47}{53}\right)$. and $\left(\frac{35}{199}\right)$.

Soln. $\left(\frac{47}{53}\right) \equiv (-1)^{\frac{46 \cdot 52}{4}} \left(\frac{53}{47}\right) \equiv (+1)\left(\frac{53}{47}\right) \equiv \left(\frac{6}{47}\right) \equiv \left(\frac{2}{47}\right)\left(\frac{3}{47}\right) \equiv 1 \cdot \left(\frac{3}{47}\right) \equiv -\left(\frac{47}{3}\right) \equiv -\left(\frac{2}{3}\right) \equiv -\left(\frac{-1}{3}\right) = -(-1) = +1$// i.e. 47 is a square mod 53. (in fact $10^2 \equiv 47$).

$\left(\frac{35}{199}\right) \equiv \left(\frac{5}{199}\right)\left(\frac{7}{199}\right) \equiv \left(\frac{199}{5}\right)(-1)\left(\frac{199}{7}\right) \equiv \left(\frac{-1}{5}\right)(-1)\left(\frac{3}{7}\right) \equiv (+1)(-1)\left(\frac{3}{7}\right) = (-1)(-1)\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$// $\because$ 1 is a square.

We can also answer questions of the form "for which primes p is a number a a square mod p?".

Ex For which primes p is -6 a square modulo p? $(p \neq 2,3)$.

soln. $\left(\frac{-6}{p}\right) \equiv \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}(-1)^{\frac{(3-1)(p-1)}{4}}\left(\frac{p}{3}\right)$. Remark: each term depends only on p modulo 24.

$\left(\frac{-6}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) \equiv (-1)^{\frac{p^2-1}{8}}\left(\frac{p}{3}\right)$. If -6 is a square mod p, $\left(\frac{-6}{p}\right) \equiv 1$, so either $(-1)^{\frac{p^2-1}{8}}$, $\left(\frac{p}{3}\right)$ are both $+1$, or both -1.

Case 1: $(-1)^{\frac{p^2-1}{8}} = +1 \Rightarrow p \equiv \pm 1\ (8)$, $p \equiv 1\ (3)$. Case 2: $(-1)^{\frac{p^2-1}{8}} = -1 \Rightarrow p \equiv \pm 3\ (8)$, $p \equiv 2\ (3)$.

p mod 24	1	5	7	11	13	17	19	23
$\left(\frac{-6}{p}\right)$	1	1	1	1	-1	-1	-1	-1

(only numbers coprime to 24). $\Rightarrow$ primes of form $p = 24k+1, 24k+5, 24k+7, 24k+11$ have -6 as a square mod p.

Primitive root testing.

Last time, we saw that $a \in \mathbb{F}_p^\times$ is a primitive root modulo $p \Leftrightarrow \forall$ primes $q \mid p-1$, $a^{\frac{p-1}{q}} \not\equiv 1 \bmod p$.

Using this method, we always need to calculate $a^{\frac{p-1}{2}} \bmod p$. But this is exactly $\left(\frac{a}{p}\right)$ by Euler's criterion. We can calculate it much quicker than before by quadratic reciprocity.

Ex Find a primitive root mod 41.

Soln. The primes dividing $41-1=40$ are 2 and 5. So we need to calculate a^{20} and a^8 mod 5. But $a^{20} \equiv \left(\frac{a}{41}\right)$ mod 41.

$\left(\frac{2}{41}\right) = 1$ since $41 \equiv \pm 1\ (8) \Rightarrow$ 2 is not a primitive root. $\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{-1}{3}\right) = -1$. $3^8 \equiv 9^4 \equiv 81^2 \equiv (-1)^2 \equiv 1\ (41) \Rightarrow$ 3 is not a primitive root.

4 is not a primitive root (obviously a square). $\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) \Rightarrow$ obvious square $\Rightarrow$ not a primitive root.

$\left(\frac{6}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{3}{41}\right) = (+1)(-1) = -1$. $6^8 \equiv 2^8 \cdot 3^8 \equiv 2^8 \cdot 1 \equiv 16^2 \equiv 256 \equiv 10\ (41)$. $10 \not\equiv 1$, so 6 is a primitive root //
$\hookrightarrow \not\equiv 1 \because 16 \not\equiv \pm 1\ (41)$.

Ex Find $\left(\frac{45}{73}\right)$.

soln. $\left(\frac{45}{73}\right) = \left(\frac{3^2 \cdot 5}{73}\right) = \left(\frac{3^2}{73}\right)\left(\frac{5}{73}\right) = \left(\frac{3}{73}\right)^2\left(\frac{5}{73}\right) = 1 \cdot \left(\frac{5}{73}\right) = \left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ // i.e. 45 is not a square mod 73.

Given an integer a, which primes p is a a square root mod p to?

- For the primes p dividing $2a$, we can answer this by hand: For these primes, a is a square modulo p.
- For all other primes p, we calculate $\left(\frac{a}{p}\right)$. the primes which we get are congruent to $4a$ i.e. we say that this depends only on $4a$.

Note: We only need to consider the numbers in $(\mathbb{Z}/24a)$ for potential values of p. Since all the other primes are going to be congruent to those.

We can solve the equations which we get from considering $\left(\frac{a}{p}\right)$ either explicitly, or by the Chinese Remainder theorem.

Ex Let $a=5$. For which primes p is a a square mod p?

Soln. First of all, we can easily answer the question for $p=2$ and $p=5$. Take $p=2$. $5 \equiv 1 \equiv 1^2$ mod 2, so 5 is certainly a square mod 2. Take $p=5$. $5 \equiv 0 \equiv 0^2$ mod 5, 5 is a square mod 5.

If $p \neq 2,5$, then we consider $\left(\frac{5}{p}\right)$. Now, $\left(\frac{5}{p}\right) = (-1)^{(5-1)(p-1)/4}\left(\frac{p}{5}\right) = (-1)^{p-1}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$; so this only depends on p modulo 5.

i.e. we are only going to consider the primes modulo 5.

p mod 5	1	2	3	4
$\left(\frac{p}{5}\right)$	1	-1	-1	1

We can read off from the table that the numbers p mod 5 for which this works are 1 or 4. So if the final answer is that 5 is a square mod p
$\Leftrightarrow p=2$ or $p=5$ or $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$.

Ex Now set $a=-5$. For which primes p is a a square root mod p?

Soln. As before, we can easily see that -5 is a square root

$\left(-\frac{5}{p}\right) = \left(-\frac{1}{p}\right)\left(\frac{5}{p}\right) = \left(-\frac{1}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right)$. Now, we know that $(-1)^{\frac{p-1}{2}}$ depends on p mod 4 and $\left(\frac{p}{5}\right)$ depends on p mod 5, so our solution depends on p mod 20.

We want either • $p \equiv 1 \pmod 4$, $p \equiv \pm 1 \pmod 5$ $\Rightarrow \left(\frac{p}{5}\right)=1$ OR • $p \equiv -1 \pmod 4$, $p \equiv \pm 2 \pmod 5$. $\Rightarrow \left(\frac{p}{5}\right) = -1$.

Note that we got this from the fact that we've already found that $\left(\frac{1}{5}\right)=1$, $\left(\frac{2}{5}\right)=-1$, $\left(\frac{3}{5}\right)=-1$, $\left(\frac{4}{5}\right)=1$; and likewise we know values of $(-1)^{\frac{p-1}{2}}$.

So, we construct the table with all the numbers up to 20 which are coprime to 20:

p mod 20	1	3	7	9	11	13	17	19
mod 4	1	-1	-1	1	-1	1	1	-1
mod 5	1	3	2	4	1	3	2	4
$\left(\frac{5}{p}\right)$	1	1	1	1	-1	-1	-1	-1

So our final answer is:

(-5) is a square modulo p if $p \equiv 1,3,7,9$ mod 20, or $p=2$, $p=5$.

Ex Set $a=-7$. For which primes p is a a square root modulo p?

Soln. For $p=2,7$, (-7) is a square root. For $p \neq 2,7$, consider $\left(\frac{-7}{p}\right)$. $\left(-\frac{7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right)(-1)^{\frac{(7-1)(p-1)}{4}}$. Now $\frac{1}{4}(7-1)(p-1) = \frac{1}{4}6(p-1) = \frac{3}{2}(p-1)$.

So $(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(7-1)(p-1)}{4}} = (-1)^{\frac{1}{2}(p-1)} \cdot (-1)^{\frac{3}{2}(p-1)} = (-1)^{2(p-1)} = 1$, so we get that $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$.

So our solutions only depend on p mod 7, and thus we need to consider the primes congruent to the numbers coprime with 7, up to 7.

We get

p	1	2	3	4	5	6
$\left(\frac{-7}{p}\right)$	1	1	-1	1	-1	-1

Since we have these values, (-7) is a square modulo p if $p=2,7$ or $p \equiv 1,2,4 \pmod 7$.

Ex Find the first primitive root mod 47.

Soln. $p-1 = 47-1 = 46 = 2 \cdot 23$, so we need to find a number a s.t. $a^2 \not\equiv 1$ mod 47, $a^{23} \not\equiv 1$ mod 47. i.e. we need to calculate $a^{23} = \left(\frac{a}{47}\right)$ mod 47, a^2 mod 47.

Then $a=2$: $2^2 = 4 \not\equiv 1$ mod 47, but $\left(\frac{2}{47}\right) = \left(\frac{47}{2}\right) = 1 \Rightarrow$ 2 is not a primitive root. $a=3$: $3^2 = 9 \not\equiv 1$ mod 47, but $\left(\frac{3}{47}\right) = -\left(\frac{47}{3}\right) = -\left(\frac{2}{3}\right) = -\left(\frac{3}{2}\right) = -\left(\frac{1}{2}\right) = 1 \Rightarrow$ 3 is not.

a=4: 4 is a square, not a primitive root. a=5: $5^2=25\not\equiv 1$ mod 47. $\left(\frac{5}{47}\right)=\left(\frac{47}{5}\right)=\left(\frac{2}{5}\right)=-1\not\equiv 1 \Rightarrow$ 5 is the first primitive root.

Ex Find the first primitive root mod 71.

Soln. $71-1=70=2\cdot5\cdot7$. So we need to calculate $a^{10}, a^{14}, a^{35}=\left(\frac{a}{71}\right)$ mod 71. For a=2, $\left(\frac{2}{71}\right)=1 \Rightarrow$ no. For a=3, $\left(\frac{3}{71}\right)=-\left(\frac{71}{3}\right)=-\left(\frac{2}{3}\right)=1\Rightarrow$ no.

a=4, 4 is a square $\Rightarrow$ no. a=5, $\left(\frac{5}{71}\right)=\left(\frac{71}{5}\right)=\left(\frac{1}{5}\right)=1\Rightarrow$ no. a=6, $\left(\frac{6}{71}\right)=\left(\frac{2}{71}\right)\left(\frac{3}{71}\right)=1\cdot1=1\Rightarrow$ no. a=7, $\left(\frac{7}{71}\right)=-\left(\frac{71}{7}\right)=-\left(\frac{1}{7}\right)=-1\Rightarrow$ yes.

Now, $7^2\equiv 49\equiv -22$ (71), $7^4\equiv 484\equiv -6$ (71), $7^8\equiv 36$ (71). Hence $7^{10}=(-35)(-22)\equiv 770\equiv 10\not\equiv 1$. $7^{14}\equiv 7^{10}\cdot 7^4\equiv 10(-6)\equiv -60\not\equiv 1$ (71)

$\therefore$ the first primitive root mod 71 is 7.

28 January 2013.
Dr. Richard M Hill
Damian LT.

The Ring $\mathbb{Z}[\xi_p]$

We will use the ring $\mathbb{Z}[\xi_p]$ in the proof of the quadratic reciprocity law.

Recall: $\mathbb{Q}[X]$ is the ring of polynomials $f(X)$ with coefficients in $\mathbb{Q}$, $\mathbb{Z}[X]$ is the ring of polynomials with coefficients in $\mathbb{Z}$.

Let $\alpha\in\mathbb{C}$. Then we use the notation $\mathbb{Q}[\alpha]=\{f(\alpha): f\in\mathbb{Q}[X]\}$, $\mathbb{Z}[\alpha]=\{f(\alpha): f\in\mathbb{Z}[X]\}$. $\mathbb{Q}[\alpha]$ and $\mathbb{Z}[\alpha]$ are rings contained in $\mathbb{C}$.

Let p be an odd prime, $\xi_p=e^{2\pi i/p}=\cos\left(\frac{2\pi}{p}\right)+i\sin\left(\frac{2\pi}{p}\right)$. We often just write ξ instead of ξ_p. $\xi_p^p=1$.

Let $m(X)=\frac{X^p-1}{X-1}=1+X+X^2+\cdots+X^{p-1}\in\mathbb{Z}[X]$. $m(\xi)=0$. We study the ring $\mathbb{Z}[\xi]$.

In fact, $\mathbb{Q}[\xi]$ is a much simpler ring, so we analyse it first.

Lemma (a) Every element $\alpha\in\mathbb{Q}[\xi]$ can be written uniquely in the form $\alpha=\sum_{n=0}^{p-2}a_n\xi^n$ $(a_n\in\mathbb{C})$

(b) $\mathbb{Q}[\xi]$ is a field.

Proof – (a) Existence: Let $\alpha=f(\xi)$ for some $f\in\mathbb{Q}[X]$. Divide f by m with remainder: $f=qm+r$, $\deg(r)<\deg(m)=p-1$; $q,r\in\mathbb{Q}[X]$.

Substitute ξ for X in this equation: $\alpha=f(\xi)=q(\xi)\overbrace{m(\xi)}^{0}+r(\xi)$. $\Rightarrow$ $\alpha=r(\xi)$ $\Rightarrow$ $\deg(\alpha)\le p-2$. q.e.d.

Uniqueness: In MATH7202, it was shown that $m(X)$ is irreducible over $\mathbb{Q}$. Suppose $\alpha=\sum_{n=0}^{p-2}a_n\xi^n=\sum_{n=0}^{p-2}b_n\xi^n$. Let $c_n=a_n-b_n$, then NTP: $\sum_{n=0}^{p-2}c_n\xi^n=0$. Let $f(X)=\sum_{n=0}^{p-2}c_nX^n$. Assume $f\not\equiv0$. Since $\deg(f)<\deg(m)$, m is irreducible $\Rightarrow$ hcf$(f,m)=1$.

By Bézout's lemma in $\mathbb{Q}[X]$, $1=hf+km$ for some $h,k\in\mathbb{Q}[X]$. Substitute $\xi=X$ in the equation. $1=h(\xi)f(\xi)+k(\xi)m(\xi)$

$m(\xi)=0$ and $f(\xi)=0$ $\Rightarrow$ $1=0$, contradiction. $\therefore f=0 \Rightarrow a_n=b_n\ \forall n \Rightarrow$ expression is unique.

(b). Choose a non-zero $\alpha\in\mathbb{Q}[\xi]$. $\alpha=f(\xi)$, $\deg(f)\le p-2$. $f\not\equiv0$. We NTP: $\frac{1}{\alpha}\in\mathbb{C}[\xi]$. f,m are coprime $\because$ m irreducible, $\deg(f)<\deg(m)$

$\therefore 1=hf+km$. Substitute ξ for X: $1=h(\xi)\underbrace{f(\xi)}_{\alpha}+k(\xi)\underbrace{m(\xi)}_{0}$ $\therefore \frac{1}{\alpha}=h(\xi)\in\mathbb{Q}[\xi]$. q.e.d.

We think of $\mathbb{Z}[\xi]$ as being a ring in $\mathbb{Q}[\xi]$ the same way that $\mathbb{Z}$ is a ring in the field $\mathbb{Q}$.

Lemma Every $\alpha\in\mathbb{Z}[\xi]$ can be written uniquely as $\alpha=\sum_{n=0}^{p-2}a_n\xi^n$. $(a_n\in\mathbb{Z})$.

Proof – (uniqueness). Already proven, follows from lemma for $\mathbb{Q}[\xi]$.

(existence). Let $\alpha=f(\xi)$ for some $f\in\mathbb{Z}[X]$. Since $\xi^p=1$, $\xi^{a+p}=\xi^a$, so we can write α in the form $\alpha=\sum_{n=0}^{p-1}a_n\xi^n$.

$m(\xi)=1+\xi+\cdots+\xi^{p-1}=0$ $\therefore \xi^{p-1}=-1-\xi-\xi^2-\cdots-\xi^{p-2}$. So we can rewrite α as $\alpha=\sum_{n=0}^{p-2}(a_n-a_{p-1})\xi^n$. q.e.d.

Ex Take p=3, $\xi=e^{\frac{2\pi i}{3}}$. Then $\mathbb{Z}[\xi]=\{a+b\xi: a,b\in\mathbb{Z}\}$ is a ring. Likewise, p=5, $\xi=e^{\frac{2\pi i}{5}}$, then $\mathbb{Z}[\xi]=\{a+b\xi+c\xi^2+d\xi^3: a,b,c,d\in\mathbb{Z}\}$ is a ring.

Definition Let $\alpha,\beta\in\mathbb{Z}[\xi]$, and let n be a positive integer. Then we say $\alpha\equiv\beta$ mod n if $\alpha-\beta=n\gamma$ for some $\gamma\in\mathbb{Z}[\xi]$.

Remark: If $\alpha=\sum_{m=0}^{p-2}a_m\xi^m$, $\beta=\sum_{m=0}^{p-2}b_m\xi^m$; then $\alpha\equiv\beta$ (n) just means $a_m\equiv b_m$ (n) (congruence in $\mathbb{Z}$!) for $m=0,1,\ldots,p-2$.

Remark: Suppose $\alpha,\beta\in\mathbb{Z}$ and n is a positive integer. Then $\alpha\equiv\beta$ (n) in $\mathbb{Z}[\xi]$ $\Leftrightarrow$ $\alpha\equiv\beta$ (n) in $\mathbb{Z}$.

$\because$ $\alpha-\beta=nc \Rightarrow c\in\mathbb{Z}[\xi]$, $c\in\mathbb{Q}$, but $\mathbb{Q}\cap\mathbb{Z}[\xi]=\mathbb{Z}$.

As a point of notation, we state that an element $\alpha\in\mathbb{Z}[\xi]$ is invertible mod n if $\exists\beta\in\mathbb{Z}[\xi]$ s.t. $\alpha\beta=1$ mod n.

Remark: If $\alpha\in\mathbb{Z}$, then if α is coprime to n in $\mathbb{Z}$, then α is invertible mod n in $\mathbb{Z}$ or in $\mathbb{Z}[\xi]$.

Lemma Let q be a prime number $\alpha,\beta\in\mathbb{Z}[\xi]$. Then $(\alpha+\beta)^q\equiv\alpha^q+\beta^q$ (this is a congruence in $\mathbb{Z}[\xi]$).

Proof – By the binomial theorem, $(\alpha+\beta)^q=\sum_{n=0}^{q}\binom{q}{n}\alpha^n\beta^{q-n}$. The first and last terms are α^q,β^q. We just must show that $\binom{q}{n}\equiv0$ (q) for $n=1,2,\ldots,q-1$. Then $\binom{q}{n}=\frac{q!}{n!(q-n)!}$. $\Rightarrow$ $q!=\binom{q}{n}n!(q-n)!$ q is prime, so q is a factor of $\binom{q}{n}$, $n!$ or $(q-n)!$. But $q\nmid n!$ and $q\nmid(q-n)!$ since these are products of numbers $<q$. $\therefore q\mid\binom{q}{n}$, and $(\alpha+\beta)^q\equiv\alpha^q+\beta^q$. q.e.d.

With these, we can begin to prove the law of quadratic reciprocity.

Definition Let p be an odd prime. The Gauss sum G_p is $G_p=\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\xi_p^n$. Remark: $G_p\in\mathbb{Z}[\xi_p]$.

$\boxed{\text{Lemma}}$ $G_p^2 = (-1)^{\frac{p-1}{2}} p$.

Proof – $G_p^2 = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\xi^a \sum_{b=1}^{p-1}\left(\frac{b}{p}\right)\xi^b = \sum_{a,b=1}^{p-1}\left(\frac{ab}{p}\right)\xi^{a+b}$. Let $b=ac$, then $G_p^2 = \sum_{a,c=1}^{p-1}\left(\frac{a^2c}{p}\right)\xi^{a+ac} = \sum_{a,c=1}^{p-1}\left(\frac{c}{p}\right)\xi^{(1+c)a}$ (a^2 is a square)

$G_p^2 = \sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\underbrace{\sum_{a=1}^{p-1}\left(\xi^{1+c}\right)^a}_{G_p} = \begin{cases}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\cdot(p-1) & \text{if } \xi=1\\ \sum_{c=1}^{p-1}\left(\frac{c}{p}\right)(\xi+\xi^2+\dots\xi^{p-1}) & \text{if } \xi\neq 1\end{cases} \Rightarrow = \underbrace{\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)}_{0}(-1) + p\times\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} p$ // q.e.d.

$\therefore m(\xi)=1$.

Recall, we earlier stated the quadratic reciprocity law: let p, q be distinct odd primes, then $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$

(QR law). Proof – We seek to calculate $(G_p)^q$ mod q in two different ways. First, $(G_p)^q = \left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\xi_p^a\right)^q \equiv \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)^q\xi_p^{aq}$ mod q. Let $b=aq$.

then $(G_p)^q \equiv \sum_{b=1}^{q-1}\left(\frac{bq^{-1}}{p}\right)\xi_p^b \equiv \left(\frac{q^{-1}}{p}\right)\sum_{b=1}^{q-1}\left(\frac{b}{p}\right)\xi_p^b \equiv \left(\frac{q}{p}\right)G_p$. mod q.

For the second calculation, we use the key lemma: $G_p^q = G_p\times(G_p^2)^{\frac{q-1}{2}} = G_p\left((-1)^{\frac{p-1}{2}}p\right)^{\frac{q-1}{2}} \equiv G_p(-1)^{\frac{(p-1)(q-1)}{4}}p^{\frac{q-1}{2}} \equiv G_p(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)$ mod q

by Euler's criterion. By comparing both calculations, $(G_p)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)(G_p)$ mod q. $G_p^2 = \pm p$ by key lemma, and p,q are

distinct primes: p is invertible mod $q \Rightarrow \therefore G_p$ is invertible mod q, we can cancel $\Rightarrow \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)$. mod q.

Both sides of equation can only take values $\pm1 \Rightarrow$ they are not just congruent mod q, they are equal $\Rightarrow \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)$ // q.e.d.

We can also use these theories to provide a proof for $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases}1 & p\equiv\pm1\ (8)\\ -1 & p\equiv\pm3\ (8)\end{cases}$

Proof – Let $\xi = e^{\frac{\pi i}{4}} = \frac{1+i}{\sqrt{2}}$. Note that $\xi^4=-1$, so let $G = \xi+\xi^7 = \xi+\xi^{-1}$. Note $G^2 = (\xi+\xi^{-1})(\xi+\xi^{-1}) = \xi^2+2\xi\xi^{-1}+\xi^{-2} = i+2-i = 2$.

We will calculate G^p mod p in two different ways in ring $\mathbb{Z}[\xi]$. First, $G^p = (\xi+\xi^{-1})^p \equiv \xi^p+\xi^{-p}$ (p) in $\mathbb{Z}[\xi]$.

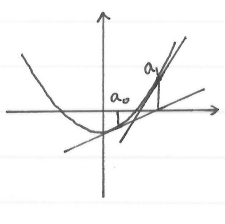
Also, $G^p = G\cdot 2^{\frac{p-1}{2}} = G\left(\frac{2}{p}\right)$ by Euler's criterion. Then $\left(\frac{2}{p}\right) \equiv \frac{\xi^p+\xi^{-p}}{\xi+\xi^{-1}}$ mod p. Since $\xi^8=1$, RHS depends only on p mod 8.

If $p=\pm1$ mod 8, $\left(\frac{2}{p}\right)=+1$; if $p=\pm3$ mod 8, $\left(\frac{2}{p}\right) \equiv \frac{\xi^3+\xi^{-3}}{\xi+\xi^{-1}} \equiv \frac{\xi^5+\xi^{-5}}{\xi+\xi^{-1}} \equiv \frac{-\xi-\xi^{-1}}{\xi+\xi^{-1}}$ $(\because \xi^4=-1) = -1$.

29 January 2013.
Dr. Richard Hill
Darwin LT.

Chapter
HENSEL's LEMMA.

Recall that if we want to solve $f(x)=0$ for a function $f:\mathbb{R}\to\mathbb{R}$, then we can try the Newton-Raphson method.



- Start with a real number a_0 s.t. $f(a_0)$ is close to 0.
- We get a better approximation to a root by the sequence $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$.

Sometimes $a_n\to a$ and $f(a)=0$.

Suppose instead that we have a polynomial $f(x)\in\mathbb{Z}[x]$, and we want to solve $f(x)\equiv 0$ (p^N), p is a prime number.

Idea: start with an "approximate root", i.e. a solution to $f(x)\equiv 0$ (p^d) where d is a small number. Call the approximate root a_0.

Define a sequence by $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$. If the method works for n big enough, $f(a_n)\equiv 0$ (p^N).

Hensel's lemma tells us when this method will work.

$\boxed{\text{EX}}$ Solve the congruence $x^2+2\equiv 0$ mod 81.

Soln. Note that $81=3^4$. There is an obvious root mod 3, $a_0=1$. $1^2+2\equiv3\equiv0$ (3). $f(x)=x^2+2$, $f'(x)=2x$

$a_{n+1} = a_n - \frac{a_n^2+2}{2a_n} = \frac{a_n}{2}-\frac{1}{a_n}$. $a_0=1$, $a_1=\frac{1}{2}-\frac{1}{1}=-\frac{1}{2}$. $a_2=-\frac{1}{4}-\frac{1}{(-\frac{1}{2})}=2-\frac{1}{4}=\frac{7}{4}$ etc. Then a_1 is a root mod 3^2, a_2 is a root mod 3^4.

$a_1=-\frac{1}{2}\equiv-2^{-1}\equiv-5\equiv4$ mod 9. Indeed $4^2+2\equiv18\equiv0$ mod 9. $a_2=\frac{7}{4}\equiv7\cdot4^{-1}\equiv7\cdot(-20)\equiv-140\equiv22$ mod 81. Indeed, $22^2+2\equiv486\equiv0$ mod 81

Note: a_3 will be a root modulo 3^8.

Remark: We have just been reducing rational numbers modulo p^n. If we have a rational number $\frac{a}{b}$, then we can reduce it mod p^n

as long as b^{-1} mod p^n exists $\Leftrightarrow$ b is coprime to p^n $\Leftrightarrow$ $p\nmid b$.

We will write $\mathbb{Z}_{(p)}$ for the set of these numbers $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a,b\in\mathbb{Z} \text{ and } p\nmid b\}$

$\boxed{\text{Lemma}}$ $\mathbb{Z}_p$ is a ring (i.e. closed under $+,\times,-$).

Proof – Let $\frac{a}{b},\frac{c}{d}\in\mathbb{Z}_{(p)}$, $p\nmid b$, $p\nmid d$. $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\in\mathbb{Z}$ $\because p\nmid bd$.

$\frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}\in\mathbb{Z}_{(p)}$, $\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}\in\mathbb{Z}_{(p)}$.

e.g. $\frac{35}{41}\in\mathbb{Z}_{(2)},\mathbb{Z}_{(3)},\dots$ but $\frac{35}{41}\notin\mathbb{Z}_{(41)}$. We defined a sequence $a_0,a_1,a_2,\dots$ we'll need to check that the sequence is contained in $\mathbb{Z}_{(p)}$

Notation: Let p be a prime and $n\in\mathbb{Z}$. Define $v_p(n)$ to be the largest integer a s.t. $p^a\mid n$. This is the ~~valuation of p at n~~. e.g. $v_2(24)=3$, $v_3(24)=1$, $v_5(24)=0$.

We define $v_p(0)=\infty$. We can extend this definition to rational numbers $v_p(\frac{a}{b})=v_p(a)-v_p(b)$. $\mathbb{Z}_{(p)}=\{x\in\mathbb{C} : v_p(x)\geq0\}$.

$\boxed{\text{Lemma}}$ (Hensel's Lemma).

Let p be prime, and let $f\in\mathbb{Z}_p[x]$. Suppose we have $a_0\in\mathbb{Z}_{(p)}$ such that $f(a_0)\equiv0$ (p^{2c+1}) where $c=v_p(f'(a_0))$.

Define a sequence $a_{n+1}=a_n-\frac{f(a_n)}{f'(a_n)}$. Then $a_n\in\mathbb{Z}_{(p)}$ for all n and $f(a_n)\equiv0$ mod p^{2c+2^n}.

Ex Solve $p=2$, $f(x)=x^2+7$.

Soln. Check that $a_0=1$ satisfies the conditions of Hensel's Lemma. $f'(a_0)=2a_0=2$ $\therefore$ $c=v_2(2)=1$. Need to check $f(a_0)\equiv 0 \bmod p^3=8$.

$f(a_0)=1^2+7=8\equiv 0\ (p^{2c+1})$. Define $a_{n+1}=a_n-\frac{a_n^2+7}{2a_n}=\frac{a_n}{2}-\frac{7}{2a_n}$. $a_1=\frac{1}{2}-\frac{7}{2}=-3$. $a_2=-\frac{3}{2}+\frac{7}{6}=-\frac{2}{6}=-\frac{1}{3}$

$a_3=-\frac{1}{6}+\frac{21}{2}=\frac{31}{3}$. $f(a_1)=a_1^2+7=9+7=16\equiv 0\ (2^4)$. $f(a_2)=(-\frac{1}{3})^2+7=\frac{1}{9}+7\equiv\frac{64}{9}\equiv 64\cdot 9^{-1}\equiv 0\ (2^6)$.

$f(a_3)=\frac{961}{9}+7\equiv\frac{1024}{9}\equiv 1024\cdot 9^{-1}\equiv 0\ (2^{10})$.

Remark: $\frac{31}{3}\equiv 31\cdot 3^{-1}\equiv 31\cdot 33\equiv 693 \bmod 1024$. Indeed, $693^2+7\equiv 0\ (1024)$.

4 February 2013.
Dr Richard M Hill.
Darwin LT.

If $x,y\in\mathbb{Z}_{(p)}$, then $x\equiv y\ (p^n) \iff v_p(x-y)\geq n$ i.e. $x-y$ is a multiple of p^n.

We prove Hensel's lemma (see page 08).

Proof – We prove by induction on n the following statements: ① $a_n\in\mathbb{Z}_{(p)}$ and $a_n\equiv a_0\ (p^{c+1})$. ② $v_p(f'(a_n))=c$. ③ $f(a_n)\equiv 0\ (p^{2c+2^n})$.

Proving these is equivalent to proving Hensel's lemma. For $n=0$, there is nothing to prove. Assume true for n and prove for $n+1$.

① $a_{n+1}=a_n-\frac{f(a_n)}{f'(a_n)}$. $a_n\in\mathbb{Z}_{(p)}$. $v_p\left(\frac{f(a_n)}{f'(a_n)}\right)=v_p(f(a_n))-v_p(f'(a_n))=v_p(f(a_n))-c$ (by inductive hypothesis ②) $\geq 2c+2^n-c$ (by inductive hypothesis ③) $\geq c+2^n$. In particular, ≥ 0 so $\frac{f(a_n)}{f'(a_n)}\in\mathbb{Z}_p \Rightarrow \frac{f(a_n)}{f'(a_n)}\equiv 0\ (p^{c+2^n}) \Rightarrow a_{n+1}\in\mathbb{Z}_{(p)}$ and $a_{n+1}\equiv a_n\ (p^{c+2^n})$

$\therefore$ $a_{n+1}\equiv a_n\ (p^{c+1})$ for $c+1<c+2^n$ $\equiv a_0\ (p^{c+1})$ by inductive hypothesis, q.e.d.

② $a_{n+1}\equiv a_0\ (p^{c+1})$ $\therefore$ $f'(a_{n+1})\equiv f'(a_n)\ (p^{c+1})$ $\therefore$ $f'(a_{n+1})\equiv f'(a_n)\ (p^c)$. We know that $f'(a_n)\equiv 0\ (p^c)$ but $\not\equiv 0\ (p^{c+1})$ by inductive hypothesis. $\therefore$ $f'(a_{n+1})\equiv 0\ (p^c)$ $\not\equiv 0\ (p^{c+1}) \Rightarrow v_p(f'(a_{n+1}))=c$, q.e.d.

③ $\frac{f(a_n)}{f'(a_n)}\equiv 0\ (p^{c+2^n})$. $a_{n+1}=a_n-\frac{f(a_n)}{f'(a_n)}$. $\therefore a_{n+1}^r\equiv\left(a_n-\frac{f(a_n)}{f'(a_n)}\right)^r\ (p^{2c+2^{n+1}})\equiv a_n^r-ra_n^{r-1}\frac{f(a_n)}{f'(a_n)}\ (p^{2c+2^{n+1}})$.

Suppose $f(x)=\sum c_r x^r$. Then $f(a_{n+1})=\sum_r c_r a_{n+1}^r=\sum_r c_r\left(a_n^r-ra_n^{r-1}\frac{f(a_n)}{f'(a_n)}\right)\ (p^{2c+2^{n+1}})=\sum_r c_r a_n^r-\left(\sum_r rc_r a_n^{r-1}\right)\frac{f(a_n)}{f'(a_n)}$

$f(a_{n+1})=f(a_n)-f'(a_n)\frac{f(a_n)}{f'(a_n)}=0.\ (p^{2c+2^{n+1}})$.

Ex Let $p=3$, and solve for a solution to $f(x)\equiv 0\ (81)$. for $f(x)=x^3+x+1$.

Soln. Take $a_0=1$. $f'(x)=3x^2+1$, $f'(a_0)=4$. $c=v_3(f'(a_0))=0$ $\because 3\nmid 4$. $f(a_0)=3\equiv 0\ (3)$, $2c+1=1$. This satisfies the conditions of Hensel's lemma. $a_{n+1}=a_n-\frac{f(a_n)}{f'(a_n)}=a_n-\frac{a_n^3+a_n+1}{3a_n^2+1}=\frac{2a_n^3-1}{3a_n^2+1}$. $a_0=1$, $a_1=\frac{2-1}{3+1}=\frac{1}{4}$. We should have $f(\frac{1}{4})\equiv 0\ (3^2)$.

Check: $\frac{1}{4}\equiv 7\equiv -2 \bmod 9$. $f(\frac{1}{4})\equiv(-2)^3+(-2)+1\equiv 0 \bmod 9$. $a_2=\frac{2\times(\frac{1}{4})^3-1}{3\times(\frac{1}{4})^2+1}=\frac{2-64}{12+64}=-\frac{62}{76}=-\frac{31}{38}$.

We should have $f(-\frac{31}{38})\equiv 0\ (3^4=81)$. Check: $38^{-1}\equiv 32\ (81)$. $\therefore a_2\equiv -31\times 32\equiv -992\equiv 61\ (81)$.

$\therefore f(a_2)\equiv(-20)^3-20+1\equiv -8000-19\equiv -8019\equiv 0\ (81)$.

__Quadratic Equations modulo n.__

Recall the Chinese Remainder theorem – If we have a congruence $f(x)\equiv 0\ (nm)$ where n and m are coprime and $f\in\mathbb{Z}[x]$, we have solutions $\iff \begin{cases} f(x)\equiv 0\ (n) \\ f(x)\equiv 0\ (m)\end{cases}$ each have solutions.

We prove this quickly: If $f(a)\equiv 0\ (nm)$ then $f(a)\equiv 0\ (n)$ and $f(a)\equiv 0\ (m)$. Conversely if $f(a)\equiv 0\ (n)$, $f(b)\equiv 0\ (m)$, then by CRT $\exists\, c\in\mathbb{Z}$ s.t. $c\equiv a\ (n)$, $c\equiv b\ (m)$. $f(c)\equiv f(a)\equiv 0\ (n)$, $f(c)\equiv f(b)\equiv 0\ (m)$. $\therefore f(c)\equiv 0\ (nm)$, q.e.d.

This means that if we want to know whether $f(x)\equiv 0\ (n)$ has solutions, where $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, p_i distinct primes, then it suffices to check whether $f(x)\equiv 0\ (p_i^{a_i})$ has solutions for every i. For a quadratic equation, it is easy to work out whether $f(x)\equiv 0\ (p^a)$ has solutions

Proposition Let p be an odd prime, and assume $a\in\mathbb{Z}$ is not a multiple of p. Then the following are equivalent:

① $x^2\equiv a\ (p)$ has solutions i.e. $(\frac{a}{p})=1$.

② $x^2\equiv a\ (p^n)$ has solutions for all n.

Proof – Let $f(x)=x^2-a$. Choose a_0 s.t. $f(a_0)\equiv 0\ (p)$, i.e. $a_0^2\equiv a\ (p)$. $f'(x)=2x$, $f'(a_0)=2a_0$, $p\nmid 2a_0$. $\therefore$ the constant c in Hensel's lemma is $c=0$. $\therefore$ a_0 satisfies the conditions of Hensel's lemma: so we get solutions $f(a_n)\equiv 0\ (p^{2^n})$ this shows ①$\Rightarrow$②. ②$\Rightarrow$① trivial, q.e.d.

Remark: This is not true for $p=2$, e.g. $a=5$. $x^2\equiv 5\ (2)$ has solution $(x=1)$ $x^2\equiv 5\ (4)$ has solutions $(x=1)$ but $x^2\equiv 5\ (8)$ has no solution.

1 is the only odd square mod 8.

Proposition Let a be an odd integer. Then the following are equivalent:

① $x^2\equiv a\ (8)$ has solutions, ② $a\equiv 1\ (8)$ ③ $x^2\equiv a\ (2^n)$ has solutions for every n.

Proof –

Now we will answer this type of question: For which n is b a square mod n? ($b \in \mathbb{Z}$).

$\boxed{\text{Ex}}$ (a) For which n is 2 a square mod n? (b) Is 5 a square?

Soln. (a) Call a prime "bad" if $p=2$ (in general, bad primes are factors of $2b$). For a "good" prime p, we know: 2 is a square mod p^n $\Leftrightarrow$ 2 is a square mod p and $\Leftrightarrow$ $\left(\frac{2}{p}\right)=1$. $\Leftrightarrow$ $p = \pm 1$ (8). For the bad prime 2, 2 is a square mod 2, but not a square mod 4, 8, 16, etc...

$\therefore$ 2 is a square mod n $\Leftrightarrow$ $n=cd$ where $c=1$ or 2, d is a product of primes $p=\pm 1$ (8) //.

For instance 2 is not a square mod $2\times 7\times 3^2\times 5^3$, but 2 is a square mod $7^{105}\times 17^{38}\times 2$.

(b) Bad primes $=\{2,5\}$. All other primes are good. For a good prime p, 5 is a square mod p^n $\Leftrightarrow$ 5 is a square mod p $\Leftrightarrow$ $\left(\frac{5}{p}\right)=1$

$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)=1$ $\Leftrightarrow$ $p\equiv 1$ or 4 mod 5. For the bad primes, 5 is a square mod 2, 4 but not mod 8. (if it was a square mod 8, it would be $\forall$ powers of 2).

5 is a square mod 5, but not mod 25. The powers of bad primes that we can have in n are factors of $4\times 5=20$. i.e. 1, 2, 4, 5, 10, 20.

Hence, 5 is a square mod n $\Leftrightarrow$ $n=ct$ where $c\in\{1,2,4,5,10,20\}$, d is product of primes ± 1 mod 5 (to any powers).

18 February 2013.
Dr. RM Hill.
Darwin LT.

Chapter
p-ADIC CONVERGENCE

Let p be a prime number. If n is an integer, then we write $v_p(n)=\max\{a : p^a | n\}$. Then $v_p(0)=\infty$.

We can extend this to $\mathbb{Q}$ by $v_p\left(\frac{n}{m}\right)=v_p(n)-v_p(m)$.

We have also defined $\mathbb{Z}_{(p)}=\left\{\frac{n}{m} : v_p\left(\frac{n}{m}\right)\geq 0\right\}$. These are the rational numbers which we can reduce modulo powers of p.

Remark: $\mathbb{Z}_{(p)}$ is closed under $+, -, \times$ so it is a ring.

Suppose we have a series $\sum_{n=0}^{\infty} x_n$, $x_n\in\mathbb{Z}_{(p)}$. We say that the series converges p-adically if $\forall a\in\mathbb{N}$, $\exists$ only finitely many terms x_n that are non-zero. i.e. $x_n \not\equiv 0$ (p^a).

Since there are only finitely many terms that are non-zero, we can reduce the whole series mod p^a. Series gives a value mod p^a (for any a).

Consider $1+p+p^2+p^3+\cdots$ Taken mod p^a, the only non-zero terms are $1+p+\cdots+p^{a-1}\equiv\frac{1}{1-p}$ (p^n). Note: this is actually $\frac{1-p^a}{1-p}$, but $p^a\equiv 0$ (p^a).

$\boxed{\text{Lemma}}$ $\sum_{n=0}^{\infty} x_n$ converges p-adically $\Leftrightarrow$ $v_p(x^n)\to\infty$.

Proof - ($\Leftarrow$). Assume $v_p(x^n)\to\infty$. Then $\exists$ N s.t. $n>N \Rightarrow v_p(x_n)>M$ i.e. $p^M | x_n$. $\Rightarrow$ $x_n\equiv 0$ (p^M).

i.e. $\exists$ only finitely many terms which are non-zero mod p^M $\Rightarrow$ $\sum_{n=0}^{\infty}x_n$ converges p-adically.

($\Rightarrow$). Assume p-adic convergence. Take any $m\in\mathbb{N}$, $\exists$ only finitely many x_n terms which are non-zero mod p^m.

Choose N large enough s.t. $x_n\equiv 0$ (p^m) $\forall$ $n>N$. $\Rightarrow$ $p^m | x_n$ $\Rightarrow$ $v_p(x_n)\geq m$ $\therefore$ $v_p(x_n)\to\infty$ // q.e.d.

$\boxed{\text{Ex}}$ Take $p=3$. The binomial expansion of $(1+3x)^{\frac{1}{2}}=1+\left(\frac{1}{2}\right)(3x)+\frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)}{2!}9x^2+\frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)}{3!}27x^3+\cdots$ Then for any $x\in\mathbb{Z}_{(3)}$, the series $(1+3x)^{\frac{1}{2}}$ converges 3-adically. The series in fact plays the same role in Number Theory as it does in Analysis (it is a square root of $1+3x$). Show this.

Soln. Clearly, $(1+3x)^{\frac{1}{2}}\equiv 1+0+0+\cdots\equiv 1$ (3). $(1+3x)^{\frac{1}{2}}\equiv 1+\frac{3}{2}x$ (9). $(1+3x)^{\frac{1}{2}}\equiv 1+\frac{3}{2}x-\frac{9}{8}x^2$ (27) etc.

We can reduce our fractions to get: $(1+3x)^{\frac{1}{2}}\equiv 1$ (3) $\equiv 1+6x$ (9) $\equiv 1+15x+9x^2$ (27).

Likewise, $(1+3x)^{\frac{1}{2}}\equiv 1+\frac{3}{2}x-\frac{9}{8}x^2+\frac{27}{16}x^3$ (27) $\equiv 1+42x+9x^2+27x^3$ (81). We can check that these are square roots of $1+3x$.

For instance, $(1+15x+9x^2)^2=1+15^2x^2+9^2x^4+2(15x+9x^2+15\cdot 9x^3)\equiv 1+3x+(18+225)x^2+0x^3+0x^4$ (27) $\equiv 1+3x$ (27) // q.e.d.

As an example, we can calculate a square root of 7 mod 81. Take $x=2$. $(1+3\cdot 2)^{\frac{1}{2}}\equiv 1+42(2)+9(4)+27(8)$ (81) $\equiv 1+3+36+54\equiv 13$.

Check: $13^2\equiv 169\equiv 2(81)+7\equiv 7$ mod 81 //.

Notation: We will write $\mathbb{Z}_{(p)}[[x]]$ for the set of power series $\sum_{n=0}^{\infty}a_nx^n$, $a_n\in\mathbb{Z}_{(p)}$. By this, we mean all power series regardless of whether they converge.

We can add, subtract and multiply power series, so $\mathbb{Z}_{(p)}[[x]]$ is a ring as well. Furthermore, we can also compose some power series.

We can compose f and g to get $f(g(x))$ as long as $g(0)=0$ i.e. $g(x)=\sum_{n=1}^{\infty}a_nx^n$. Let $f(x)=\sum_{n=0}^{\infty}a_nx^n$, $g(x)=\sum_{m=1}^{\infty}b_mx^m$

We'll see that $f(g(x))$ is also a power series in $\mathbb{Z}_{(p)}[[x]]$. Then $f(g(x))=\sum_{n=0}^{\infty}a_n\,g(x)^n=\sum_{n=0}^{\infty}a_n\left(\sum_{m=1}^{\infty}b_mx^m\right)^n=\sum_{n=0}^{\infty}a_n\sum_{m_1,m_2,\ldots,m_n=1}^{\infty}b_{m_1,m_2,\ldots,m_n}x^{m_1+\cdots+m_n}$

This can be re-expressed as $\sum_{d=0}^{\infty}c_dx^d$ where $c_d=\sum_{\substack{n,\,m_1+\cdots+m_n\\=d}}a_n b_{m_1}b_{m_2}\cdots b_{m_n}$ where each $m_i>0$. Since the sum defining c_d is finite, it converges and is in $\mathbb{Z}_{(p)}$. $\therefore$ $f(g(x))\in\mathbb{Z}_{(p)}[[x]]$.

i.e. we can compose power series in $\mathbb{Z}_{(p)}[[x]]$ as long as $x | g(x)$.

$\boxed{\text{Lemma}}$ (the Power series trick).

Suppose we have $f, g, h \in \mathbb{Z}_{(p)}[[x]]$. Assume that

- for all $x \in \mathbb{Z}_{(p)}$, $f(x), g(x), h(x)$ converge periodically,
- for any $x \in \mathbb{R}$ sufficiently small, $f(x), g(x), h(x)$ converge and $h(x) = f(g(x))$.

Then for any a, and any $x \in \mathbb{Z}_{(p)}$, $\quad f(g(x)) \equiv h(x) \mod p^a$.

Note: In the example $(1+3x)^{\frac{1}{2}}$, $f(x) = x^2$, $g(x) = (1+3x)^{\frac{1}{2}}$, $h(x) = 1+3x$. For small $x \in \mathbb{R}$, $((1+3x)^{\frac{1}{2}})^2 = 1+3x$.

The lemma tells us that the same is true mod p^a for every a. In order to use the lemma for the example $(1+3x)^{\frac{1}{2}}$, we need to check that this converges p-adically for all $x \in \mathbb{Z}_{(p)}$.

$\boxed{\text{Lemma}}$ $v_p(n!) \leq \frac{n}{p-1}$.

Proof – $v_p(n!) = v_p(1) + v_p(2) + \cdots + v_p(n)$. Then $\lfloor \frac{n}{p} \rfloor$ of the numbers $1, \dots, n$ are multiples of p, $\lfloor \frac{n}{p^2} \rfloor$ of the numbers $1, \dots, n$ are multiples of p^2.

$\therefore \lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor$ gives the numbers from $1, \dots, n$ that are multiples of p but not p^2 (i.e. valuation is 1). Similarly,

$\lfloor \frac{n}{p^2} \rfloor - \lfloor \frac{n}{p^3} \rfloor$ of $1, \dots, n$ are multiples of p^2 but not p^3 etc. $\therefore v_p(n!) = (\lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor)(1) + (\lfloor \frac{n}{p^2} \rfloor - \lfloor \frac{n}{p^3} \rfloor)(2) + \cdots\cdots$

We rearrange to give $v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor (2-1) + \lfloor \frac{n}{p^3} \rfloor (3-2) + \cdots = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor \leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{n}{p}(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots) = \frac{n}{p} \cdot \frac{1}{1-\frac{1}{p}} = \frac{n}{p-1}$ // q.e.d

Now, we look again at our example $(1+3x)^{\frac{1}{2}} = 1 + (\frac{1}{2}) 3x + \frac{(\frac{1}{2})(-\frac{1}{2})}{2!} 9x^2 + \cdots$. The n^{th} term is $\frac{(\frac{1}{2})(\frac{1}{2}-1)\cdots(\frac{1}{2}-n+1)}{n!} 3^n x^n$.

To show that the series converges p-adically, we just need to show that $v_p(n^{th}\text{ term}) \to \infty$. Take $p=3$. Then we evaluate $v_3(n^{th}\text{ term})$.

$$v_3(n^{th}\text{ term}) = \underbrace{v_3(\tfrac{1}{2}) + v_3(\tfrac{1}{2}-1) + v_3(\tfrac{1}{2}-2) + \cdots + v_3(\tfrac{1}{2}-n+1)}_{\text{rational, no 3 in denominator}} + n + n\underbrace{v_3(x)}_{x \in \mathbb{Z}_{(p)}} - v_3(n!) \geq 0 + 0 + \cdots + 0 + n + n(0) - \frac{n}{3-1} = n - \frac{n}{3-1} = \frac{n}{2}.$$

Hence, $v_3(n^{th}\text{ term}) \geq \frac{n}{2}$ i.e. $v_3(n^{th}\text{ term}) \to \infty$ as $n \to \infty \Rightarrow$ series converges p-adically.

We now move on to prove the power series trick stated above.

Proof – let $f(x) = \sum_{n=0}^{\infty} a_n x^n$, $g(x) = \sum_{m=1}^{\infty} b_m x^m$, $h(x) = \sum_{n=0}^{\infty} c_n x^n$. We know that for small $x \in \mathbb{R}$, $h(x) = f(g(x))$.

By uniqueness of power series expansions, $\quad c_d = \sum_{m_1 + \cdots + m_n = d} a_n b_{m_1} b_{m_2} \cdots b_{m_n}$.

Since the series converges p-adically, $\exists N$ s.t. if $n > N$, $m > N$, then $a_n, b_m \equiv 0 \ (p^a)$. Let $f_0(x) = \sum_{n=0}^{N} a_n x^n$, $g_0(x) = \sum_{m=1}^{N} b_m x^m$. These are polynomials, and $f_0(g_0(x)) = \sum c'_d x^d$ where $c'_d = \sum_{m_1 + \cdots + m_n = d} a_n b_{m_1} \cdots b_{m_n}$, $0 \leq n \leq N$, $0 < m_i \leq N$.

The difference between c_d and c'_d is just some terms which are 0 mod p^a, i.e. $c_d \equiv c'_d \mod (p^a)$, i.e. $h(x) \equiv \sum c_d x^d \ (p^a)$.

Then $h(x) \equiv \sum c'_d x^d \ (p^a) \equiv f_0(g_0(x)) \ (p^a)$ but $f_0(x) \equiv f(x)$, $g_0(x) \equiv g(x) \ (p^a)$, so $h(x) \equiv f(g(x)) \ (p^a)$ // q.e.d.

19 February 2013.
Dr. Richard M HILL.
Damin H.

$\boxed{\text{Definition}}$ Let p be an odd prime. We write $p\mathbb{Z}/p^n$ for the elements of $\mathbb{Z}/p^n$ which are multiples of p.

e.g. $3\mathbb{Z}/3^3 = 3\mathbb{Z}/27 = \{0, 3, 6, \dots, 21, 24\}$. $p\mathbb{Z}/p^n$ is closed under $+$, and is an additive subgroup of $\mathbb{Z}/p^n$ with p^{n-1} elements.

We write $1 + p\mathbb{Z}/p^n$ for the elements $1 + px$, where $x \in \mathbb{Z}/p^n$ i.e. these are the elements of $\mathbb{Z}/p^n$ which are congruent to 1 (mod p)

e.g. $1 + 3\mathbb{Z}/3^3 = \{1, 4, 7, 10, \dots, 22, 25\}$. $1 + p\mathbb{Z}/p^n$ is closed under $\times$, and is a multiplicative subgroup of $(\mathbb{Z}/p^n)^\times$ with p^{n-1} elements.

We will eventually establish that $p\mathbb{Z}/p^n \cong 1 + p\mathbb{Z}/p^n$.

$\boxed{\text{Proposition}}$ For any odd prime p, the exponential power series $\exp(px) = 1 + px + \frac{(px)^2}{2!} + \frac{(px)^3}{3!} + \cdots$ converges p-adically for any $x \in \mathbb{Z}_{(p)}$.

Proof – NTP: $v_p(\text{general term}) \to \infty$. So we have $v_p(\frac{p^n x^n}{n!}) = v_p(p^n) + v_p(x^n) - v_p(n!) = n\underbrace{v_p(p)}_{=1} + n\underbrace{v_p(x)}_{\geq 0} - \underbrace{v_p(n!)}_{\leq \frac{n}{p-1}} \geq n - \frac{n}{p-1} = n(\frac{p-2}{p-1})$.

Since p is an odd prime, $p \neq 2$. $p \geq 3 \Rightarrow p-2 > 0$ i.e. $n \cdot (\frac{p-2}{p-1}) \to \infty$ as $n \to \infty$ // q.e.d.

Now we consider the logarithmic series. Recall that $1 + x + x^2 + \cdots = \frac{1}{1-x}$, $1 - x + x^2 - \cdots = \frac{1}{1+x}$. Since $\int \frac{dx}{1+x} = \log(1+x)$, we integrate term by term: $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$

$\boxed{\text{Proposition}}$ For any odd prime p, the $\log(1+x)$ power series $\log(1+px) = px - \frac{(px)^2}{2} + \frac{(px)^3}{3} - \frac{(px)^4}{4} + \cdots$ converges p-adically $\forall x \in \mathbb{Z}_{(p)}$.

Proof – General term of series is $\frac{p^n x^n}{n}$. Then $v_p(\frac{p^n x^n}{n}) = n\underbrace{v_p(p)}_{=1} + n\underbrace{v_p(x)}_{\geq 0} - \underbrace{v_p(n)}_{\leq \log_p(n)}$. Suppose $v_p(n) = c$, then $p^c \mid n$. $n = mp^c$. Take $\log p$ both sides:

$\log_p(n) = c \log_p(m) \Rightarrow c = \frac{\log_p(n)}{\log_p(m)} \leq \log_p(n)$. Hence, $v_p(\frac{p^n x^n}{n}) \geq n - \log_p(n) \to \infty$ as $n \to \infty$ // q.e.d.

$\boxed{\text{Theorem}}$ $p\mathbb{Z}/p^n \cong 1 + p\mathbb{Z}/p^n$ are isomorphic, with isomorphism $px \mapsto \exp(px)$, $\log(1+py) \leftarrow 1 + py$.

Proof – We have already shown that power series for $\log(1+px)$ and $\exp(px)$ converge p-adically. Also, for small $x \in \mathbb{R}$, exp and log are inverse functions.

$\therefore$ From power series trick, $\exp(\log(1+py)) \equiv (1+py) \pmod{p^n}\ \forall n$, $\log(\exp(px)) \equiv px \pmod{p^n}\ \forall n$. In particular, there is a bijection between them.

Only remains to show homomorphism: $\exp(p(x+y)) \equiv \sum_{m=0}^{\infty} p^m \frac{(x+y)^m}{m!} \equiv \sum_{m=0}^{N} p^m \frac{(x+y)^m}{m!} \pmod{p^n}$ for N sufficiently large. So,

$\sum_{m=0}^{N} \frac{p^m}{m!} \sum_{a=0}^{m} \frac{m!}{a!(m-a)!} x^a y^{m-a} \quad (p^n) \equiv \sum_{a=0}^{N} \frac{1}{a!} \sum_{b=0}^{N} \frac{1}{b!} (px)^a (py)^b$ for $b = m-a$ $= \sum_{a=0}^{N} \frac{1}{a!} \sum_{b=0}^{N} \frac{1}{b!} (px)^a (py)^b = \exp(px)\exp(py) \pmod{p^n}$ // q.e.d.

Remark: If $a \in \mathbb{Z}_{(p)}$ and $a \equiv 1 \pmod p$, we can define a^b for all $b \in \mathbb{Z}_{(p)}$ p-adically i.e. we can define this modulo p^n for every n.

Definition $a^b = \exp(b \log a)$ i.e. $a^b \equiv \exp(b \log a) \mod p^n \ \forall n$.

Ex Expand mod 27, $\exp(3x)$ and $\log(1+3x)$. Check that $\log(\exp(3x)) \equiv 3x \pmod{27}$.

Soln. $27 = 3^3$. $\exp(3x) \equiv 1 + 3x + \frac{9}{2}x^2 + \frac{27}{6}x^3 \equiv 1 + 3x + 18x^2 + 18x^3 \pmod{27}$, $\log(1+3x) \equiv 3x - \frac{9x^2}{2} + \frac{27}{3}x^3 \equiv 3x + 9x^2 + 9x^3 \pmod{27}$.

$\log(\exp(3x)) \equiv \log(1 + 3x + 18x^2 + 18x^3) \equiv \log(1 + 3(x + 6x^2 + 6x^3)) \equiv 3(x+6x^2+6x^3) + 9(x+6x^2+6x^3)^2 + 9(x+6x^2+6x^3)^3 \pmod{27}$.

The expressions $(x+6x^2+6x^3)^2$ and $(x+6x^2+6x^3)^3$ are multiplied by 9. To find them mod 27, we only need to find them mod 3.

Expanding, only non-zero elements are x^2, x^3, hence $\Rightarrow \log(\exp(3x)) \equiv 3x + 18x^2 + 18x^3 + 9x^2 + 9x^3 + 0 \equiv 3x$ q.e.d.

We can use this to calculate 4^x 3-adically: i.e. $4^x \pmod{27}$, as $4 \equiv 1 \pmod 3$. We can use the result from the previous remark:

$\log(4) \equiv \log(1 + 3 \times 1) \equiv 3 + 9 + 9 \equiv 21 \equiv -6 \pmod{27}$ $\therefore 4^x \equiv \exp(x \log(4)) \equiv \exp(-6x) \equiv 1 - 6x + \frac{36}{2}x^2 - \frac{216}{6}x^3 \equiv 1 - 6x + 18x^2 - 9x^3 \equiv 1 - 6x - 9x^2 - 9x^3 \pmod{27}$.

So, for example, when $x = \frac{1}{2}$, $1 - \frac{6}{2} - \frac{9}{4} - \frac{9}{8} \equiv 1 - 3 - \frac{9}{4} - \frac{9}{8} \equiv 1 - 3 - 9(\frac{1}{4} + \frac{1}{8}) \equiv 1 - 3 \equiv -2 \pmod{27}$. So $4^{\frac{1}{2}} \equiv -2 \pmod{27}$.

25 February 2013
Dr. Richard M Hill.
Darwin LT.

Teichmüller Lifts.

Last time we saw that $1 + p\mathbb{Z}/p^n \cong p\mathbb{Z}/p^n \cong \mathbb{Z}/p^{n-1}$. So we understand completely the subgroup $1 + p\mathbb{Z}/p^n$ of $(\mathbb{Z}/p^n)^\times$.

Today we will find another group G s.t. $(\mathbb{Z}/p^n)^\times \cong G \times (1 + p\mathbb{Z}/p^n)$. G is called the group of Teichmüller lifts.

Let $x \in \mathbb{Z}_{(p)}$ with $x \not\equiv 0$ (p). By Fermat's little theorem, $x^{p-1} \equiv 1 \mod p$, $\therefore x \equiv x^p \equiv (x^p)^p \equiv ((x^p)^p)^p \equiv \cdots \equiv x \pmod p$. i.e. the sequence $x, x^p, x^{p^2}, \ldots$ is constant mod p. It will turn out that the sequence is eventually constant mod p^d for any d.

Definition The Teichmüller lift $T(x)$ of x mod p^d is $T(x) \equiv x^{p^{d-1}} \mod p^d$, i.e. $T(x) \in \mathbb{Z}/p^d$.

Note: We assume that p is an odd prime $(p \neq 2)$ when discussing Teichmüller lifts.

Lemma Suppose $T(x) \equiv a$ (p^n). Then $T(x) \equiv a^p$ (p^{n+1}).

Proof – If $T(x) \equiv a$ (p^n), then $T(x) = a + p^n b$ for some b. $T(x) \equiv (a + p^n b)^p \mod p^{n+1} \equiv a^p + p a^{p-1} p^n b + \cdots \equiv a^p$ (p^{n+1}). mod p^{n+1}.

Ex Calculate $T(2)$ mod $125 = 5^3$.

Soln. $T(2) \equiv 2^{5^{2-1}}$ (5^2) $\equiv 2^5$ (5^2) $\equiv 32$ (25) $\equiv 7$ (25) $\therefore T(2) \equiv 7^5 \pmod{125}$ (by Lemma above) $\equiv (2+5)^5$

By Binomial theorem, $7^5 \equiv 2^5 + 5(2^4)(5) + \overbrace{10(2^3)(5^2)}^{2^4 \cdot 5^3} + \cdots \equiv 2^5 + 5^2 \times (\underbrace{2^4}_{\text{take mod } 5}) \equiv 32 + 5^2 \cdot 1 \equiv 32 + 25 \equiv 57 \pmod{125}$

Theorem Let p be an odd prime. Then,

① $\forall r > n-1$, $T(x) \equiv x^{p^r} \mod p^n$, ② $T(x)^{p-1} \equiv 1 \mod p^n$ ③ $T(x)$ only depends on x mod p and $T(x) \equiv x$ mod p. ④ $T : \mathbb{F}_p^\times \to (\mathbb{Z}/p^n)^\times$ is an injective homomorphism

Proof – By Euler's theorem, $\varphi(p^n) = (p-1)p^{n-1} \Rightarrow x^{(p-1)p^{n-1}} \equiv 1 \mod p^n \Rightarrow T(x)^{p-1} \equiv 1$ (p^n) $\Rightarrow$ ② q.e.d. Consider that

$(x^{p^{n-1}})^{p-1} \equiv 1 \Rightarrow (x^{p^{n-1}})^p \equiv x^{p^{n-1}} \mod p^n$. Then $x^{p^n} \equiv x^{p^{n-1}} \mod p^n \Rightarrow$ ① q.e.d. Suppose $x \equiv y \mod p \Rightarrow \frac{x}{y} \equiv 1 \mod p$. $\equiv \exp(pz) \mod p^n$

$\frac{T(x)}{T(y)} \equiv \exp(pz)^{p^{n-1}} \pmod{p^n} \equiv \exp(p^{n-1} pz) \equiv \exp(p^n z) \equiv \exp(0 \cdot z) \equiv 1 \pmod{p^n} \Rightarrow T(x) = T(y) \Rightarrow T(x)$ only depends on x mod p q.e.d.

$x \equiv x^p \equiv x^{p^2} \equiv \cdots \equiv x^{p^{n-1}}$ (mod p) by Fermat's little theorem $\Rightarrow$ ③ q.e.d. Finally, we show that T is a homomorphism:

$T(xy) = (xy)^{p^{n-1}} \equiv x^{p^{n-1}} y^{p^{n-1}} = T(x)T(y)$. For injectivity, suppose $T(x) \equiv T(y) \mod p^n$. $\therefore T(x) \equiv T(y) \mod p \Rightarrow x \equiv y \mod p$, by ③.

So $x \equiv y$ (mod p) q.e.d.

Ex We have already shown that $T(2) \equiv 57 \pmod{125}$. Find all Teichmüller lifts modulo 125.

Soln. $T(1) \equiv 1$ (125), $T(2) \equiv 57$ (125), $T(4) \equiv T(-1) \equiv -1 \equiv 124$ (125) $T(3) \overset{\text{(homomorphism)}}{\equiv} T(-1)T(2) \equiv -57 \equiv 68 \mod 125$.

x mod 5	1	2	3	4
T(x) mod 125	1	57	68	124.

These form a subgroup of $(\mathbb{Z}/125)^\times$. It is the image of $T : \mathbb{F}_5^\times \to (\mathbb{Z}/125)^\times$.

Corollary Let p be an odd prime. Every element $a \in (\mathbb{Z}/p^n)^\times$ can be written uniquely as $a = T(x) \cdot \exp(py)$ for $x \in \mathbb{F}_p^\times$, $y \in \mathbb{Z}/p^{n-1}$. i.e. $(\mathbb{Z}/p^n)^\times \cong \mathbb{F}_p^\times \times \mathbb{Z}/p^{n-1}$.

Proof – (Existence) Let $x \equiv a$ mod p, $T(x) \equiv a$ (p) $aT(x)^{-1} \equiv 1$ (p). Let $py = \log(aT(x)^{-1})$ (p^n). $\therefore a = T(x)\exp(py)$.

(Uniqueness) Suppose $T(x)\exp(py) \equiv T(x')\exp(py') \mod p^n$. $\exp(py) \equiv \exp(py') \equiv 1$ (p) $\Rightarrow T(x) \equiv T(x')$ (p) $\Rightarrow x = x' \mod p$

$\therefore \exp(py) \equiv \exp(py')$. Take logarithms: $\therefore py \equiv py'$ (p^n) $\Rightarrow y \equiv y'$ (p^{n-1}) q.e.d.

Ex Write 22 as $T(x)\exp(py)$ mod 125. Then evaluate 22^{37} mod 125.

Soln. $22 \equiv T(x)\exp(py)$ (125) $\Rightarrow 2 \equiv x \pmod 5$. $22 \equiv T(2)\exp(py)$. $\exp(py) \equiv 22 \cdot [T(2)]^{-1} \overset{\text{homomorphism}}{\equiv} 22\, T(2^{-1}) \equiv 22\, T(3) \equiv 22 \cdot 68 \pmod{125}$

$\exp(py) \equiv 1496 \equiv 121 \equiv -4 \pmod{125}$. $py \equiv \log(-4) \equiv \log(1-5) \equiv -5 - \frac{25}{2} + \cdots \equiv -5 - 25(\underbrace{3}_{\text{inverse } 2^{-1} \text{ mod } 5}) \equiv -80 \pmod{125} \equiv 45$.

Then $22 \equiv T(2)\exp(45) \equiv T(2)\exp(5 \times 9)$. Therefore, we can calculate $22^{37} \equiv T(\underbrace{2^{37}}_{2^4 \equiv 1})\exp(37 \times 45) \equiv T(2)\exp[5 \times (\underbrace{37 \times 9}_{\text{take mod } 25})] \mod 125$

$\equiv T(2)\exp[5 \times 12 \times 9] \equiv T(2)\exp[5 \times 8] \equiv T(2)\exp(40) \equiv 57 \times (1 + 40 + \frac{40^2}{2}) \equiv 57 \times 841 \equiv 57 \times (-34) \equiv -1938 \equiv 62 \pmod{125}$.

Chapter 5

GAUSSIAN INTEGERS.

Definition A Gaussian integer is a complex number of the form $x+iy$ $(x,y \in \mathbb{Z})$. These form a ring, and we write $\mathbb{Z}[i]$ for this ring $(i^2=-1)$.

$\mathbb{Z}[i]$ is contained in the field $\mathbb{Q}[i] = \{x+iy : x,y \in \mathbb{Q}\}$.

We use the notation $N(x+iy) = x^2+y^2$ to denote the norm of $x+iy$. Note: $N(x+iy) = (x+iy)(x-iy)$, i.e. $N(\alpha) = \alpha\bar{\alpha}$ $\forall\, \alpha \in \mathbb{Z}[i]$, where $\bar{\alpha}$ is the complex conjugate of α.

From this, we get $N(\alpha\beta) = N(\alpha)N(\beta)$. In general for a ring R, we write $R^\times$ for the invertible elements in R i.e. $R^\times \{x \in R : \exists\, y \in R \text{ s.t. } xy=1\}$.

Lemma $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Proof - Suppose α is invertible, then $N(\alpha)N(\alpha^{-1}) = N(1) = 1$. But $N(\alpha), N(\alpha^{-1})$ are +ve integers $\therefore N(\alpha) = N(\frac{1}{\alpha}) = 1$. If $\alpha = x+iy$, $N(\alpha) = x^2+y^2$, so $\alpha = \pm 1$ or $\pm i$ // q.e.d

Definition Let $\alpha, \beta \in \mathbb{Z}[i]$. An element $\gamma \in \mathbb{Z}[i]$ is a highest common factor of α and β if

- $\gamma | \alpha$ and $\gamma | \beta$ in $\mathbb{Z}[i]$ (i.e. $\frac{\alpha}{\gamma}, \frac{\beta}{\gamma} \in \mathbb{Z}[i]$), and
- if $\delta | \alpha$, $\delta | \beta$, then $N(\delta) \le N(\gamma)$.

Remark: If γ is a highest common factor of α, β, then $i\gamma, -\gamma, -i\gamma$ are also highest common factors (i.e. there are four).

There is a version of the Euclidean algorithm for $\mathbb{Z}[i]$.

Lemma Let $\alpha, \beta \in \mathbb{Z}[i]$ $(\beta \ne 0)$. Then $\exists\, Q, R \in \mathbb{Z}[i]$ s.t. $\alpha = Q\beta + R$ and $N(R) \le \frac{1}{2}N(\beta)$.

Proof - Let $\frac{\alpha}{\beta} = x+iy \in \mathbb{C}$. Choose integers a, b s.t. $|x-a| \le \frac{1}{2}$, $|y-b| \le \frac{1}{2}$. Clearly, a, b are well-defined. Let $Q = a+ib$.

$\frac{\alpha}{\beta} - Q = (x-a)+i(y-b)$. Then $N(\frac{\alpha}{\beta}-Q) = (x-a)^2+(y-b)^2 \le (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$. Let $R = \alpha - Q\beta$. Then $N(R) = N(\alpha - Q\beta) = N(\beta)N(\frac{\alpha}{\beta}-Q) \le \frac{1}{2}N(\beta)$ // q.e.d.

Remark: If $\alpha = Q\beta + R$, then the common factors of α and β are the same as the common factors of β and R. $\therefore \operatorname{hcf}(\alpha,\beta) = \operatorname{hcf}(\beta, R)$.

Thus, we can calculate $\operatorname{hcf}(\alpha,\beta)$ by an iterative process exactly as in $\mathbb{Z}$ by Euclidean algorithm.

Ex Take $\alpha = 8+10i$, $\beta = 3+2i$. Find $\operatorname{hcf}(\alpha,\beta)$.

Soln. $\frac{\alpha}{\beta} = \frac{(8+10i)(3-2i)}{(3+2i)(3-2i)} = \frac{1}{13}[24-16i+30i+20] = \frac{44}{13} + i\frac{14}{13} = (3+\frac{5}{13}) + i(1+\frac{1}{13})$. Take $Q = 3+i$. $R = \alpha - Q\beta = 8+10i - (3+i)(3+2i) = (8+10i) - (9+6i+3i-2)$.

Then $R = 8+10i - (9i-7) = 1+i$. Hence, $\underset{\alpha}{(8+10i)} = (3+i)\underset{\beta}{(3+2i)} + \underset{R}{(1+i)}$. Then $\frac{3+2i}{1+i} = \frac{(3+2i)(1-i)}{(1+i)(1-i)} = \frac{1}{2}(3-3i+2i+2) = \frac{5}{2} - \frac{1}{2}i$. Take $Q = 2$.

then $(3+2i) = 2(1+i)+1$. then $\frac{1+i}{1} = 1+i \Rightarrow (1+i) = (1+i)(1) + \underset{R}{0} \Rightarrow \operatorname{hcf}(\alpha,\beta) = \operatorname{hcf}(8+10i, 3+2i) = 1$. (or $i, -1, -i$).

Exactly as in $\mathbb{Z}$, we have a variant of Bézout's lemma:

Lemma $\exists\, H, K \in \mathbb{Z}[i]$ s.t. $\operatorname{hcf}(\alpha,\beta) = H\alpha + K\beta$.

26 February 2013.
Dr. Richard M Hill.
Darvin LT.

Ex (cont'd) Express $1 = H(8+10i) + K(3+2i)$, finding K and H.

Soln. $1 = (3+2i) - 2(1+i) = (3+2i) - 2((8+10i) - (3+i)(3+2i)) = (1+2(3+i))(3+2i) - 2(8+10i) = (7+2i)(3+2i) - 2(8+10i)$.

so $H = -2$, $K = 7+2i$.

Definition An element π is called a Gaussian prime, if

① $N(\pi) \ge 2$, ② If $\pi = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i]$, then $\alpha \in \mathbb{Z}[i]^\times$ or $\beta \in \mathbb{Z}[i]^\times$.

Lemma Let π be a Gaussian prime. Suppose $\pi | \alpha\beta$. Then $\pi | \alpha$ or $\pi | \beta$.

Proof - Assume $\pi \nmid \alpha$, then $\operatorname{hcf}(\pi, \alpha) = 1$. $\exists\, H, K \in \mathbb{Z}[i]$ s.t. $1 = H\pi + K\alpha$ $\therefore \beta = H\pi\beta + K\alpha\beta$. Since $\pi | \alpha\beta$, $\pi | \text{RHS} \Rightarrow \pi | \text{LHS} \Rightarrow \pi | \beta$ // q.e.d.

Using this, we can also prove:

Theorem (Uniqueness of Factorisation).

Let $\alpha \in \mathbb{Z}[i]$, $\alpha \ne 0$. Then $\exists$ Gaussian primes $\pi_1, \dots, \pi_n$ s.t. $\alpha = \pi_1 \cdots \pi_n$. If $\alpha = \varphi_1 \cdots \varphi_m$ (φ_i prime) then $n = m$ and we can reorder the φ_i s.t. $\frac{\pi_i}{\varphi_i} \in \mathbb{Z}[i]^\times$

Lemma Let π be any Gaussian prime. Then $\exists$ unique prime $p \in \mathbb{Z}$ s.t. $\pi | p$.

Proof - Let $n = \pi\bar{\pi} = N(\pi)$. $\therefore \pi | n$ but $n \in \mathbb{Z}$, so we can factorise n into primes in $\mathbb{Z}$. $n = p_1 \cdots p_r$. By the lemma, $\pi | p_i$ for some i.

For uniqueness, suppose $\pi | p$ and $\pi | q$ with p, q coprime. $\operatorname{hcf}(p,q) = 1$. $1 = hp + kq$ for some $h, k \in \mathbb{Z}$. $\therefore \pi | hp + kq = 1 \Rightarrow$ contradiction // q.e.d.

This tells us that in order to find all the Gaussian primes, we need to factorise each prime $p \in \mathbb{Z}$ into Gaussian primes.

Suppose p is a prime with $\mathbb{Z}$; with a factorisation $p = \pi_1 \cdots \pi_r$ into Gaussian primes.

$N(p) = p^2$ $\therefore p^2 = N(\pi_1)N(\pi_2) \cdots N(\pi_m)$; $N(\pi_i) \ge 2$. This then shows one of three cases:

① $p = \pi_1\pi_2$ with $N(\pi_1) = N(\pi_2) = p$ and $\frac{\pi_1}{\pi_2} \notin \mathbb{Z}[i]^\times$ — p is split in $\mathbb{Z}[i]$

② p is a Gaussian prime itself with norm p^2. — p is inert in $\mathbb{Z}[i]$

③ $p = n\pi^2$ where π is a Gaussian prime with norm p and $n \in \mathbb{Z}[i]^\times$. — p is ramified in $\mathbb{Z}[i]$

For example: $2 = -i(1+i)^2$ (2 is ramified). 3 is inert (does not factorise). $5 = (2+i)(2-i)$, so 5 is split in $\mathbb{Z}[i]$.

Theorem (Decomposition theorem for Gaussian integers)

① $2=(-i)(1+i)^2$, so 2 is ramified. ② If $p\equiv 1 \bmod 4$, p is split in $\mathbb{Z}[i]$. ③ If $p\equiv 3 \bmod 4$, p is inert in $\mathbb{Z}[i]$.

e.g. $37\equiv 1\ (4)$: $37=(6+i)(6-i)$. $41\equiv 1\ (4)$: $41=(5+4i)(5-4i)$.

Proof – ① is clearly true. For ③, suppose $p\equiv 3 \pmod 4$. Suppose $\exists$ Gaussian prime of norm p.

$\pi = x+iy \Rightarrow x^2+y^2=p$, $x^2+y^2\equiv 3 \pmod 4$. But the squares mod 4 are $0^2\equiv 0$, $1^2\equiv 1$, $2^2\equiv 0$, $3^2\equiv 1 \pmod 4$.

Hence, $x^2+y^2=N\equiv 3 \Rightarrow$ contradiction. For ②, suppose $p\equiv 1 \pmod 4$ by quadratic reciprocity. -1 is a quadratic residue modulo p.

choose $a\in\mathbb{Z}$ s.t. $a^2\equiv -1\ (p)$. i.e. $a^2+1\equiv 0 \pmod p$. Let $\alpha=a+i$. then $\alpha\bar{\alpha}=a^2+1\equiv 0 \pmod p$. so $p\mid\alpha\bar{\alpha}$.

Let $\pi = \mathrm{hcf}(\alpha,p)$, $\bar{\pi}=\mathrm{hcf}(\bar{\alpha},p)$. since $\pi\mid p$, we know $N(\pi)\mid p^2$ $\therefore N(\pi)=1$ or p or p^2.

α and $\bar{\alpha}$ are not both coprime to p $\because p\mid\alpha\bar{\alpha}$, so either π or $\bar{\pi}$ is not in $\mathbb{Z}[i]^\times$ $\therefore$ neither π nor $\bar{\pi}$ are in $\mathbb{Z}[i]^\times$.

If $N(\pi)=p^2$ and $\pi\mid p$, then $p/\pi\in\mathbb{Z}[i]^\times$ since its norm is 1. $\therefore p\mid\alpha \Rightarrow a+i\mid\alpha \Rightarrow$ clearly contradiction. $\therefore N(p)=p$, $p=\pi\bar{\pi}$.

Remains to check that $\pi/\bar{\pi}\notin\mathbb{Z}[i]^\times$, i.e. π and $\bar{\pi}$ are coprime. Suppose $\beta\mid\pi$ and $\beta\mid\bar{\pi}$. $\therefore \beta\mid\alpha, \beta\mid\bar{\alpha}, \beta\mid p$.

$\therefore \beta\mid\alpha-\bar{\alpha}=2i \Rightarrow \beta\mid 2$. choose h,k s.t. $1=2h+pk$ $\because \mathrm{hcf}(2,p)=1$. $\therefore \beta\mid 2, \beta\mid p \Rightarrow \beta\mid 1$. $\therefore \mathrm{hcf}(\pi,\bar{\pi})=1$ q.e.d.

4 March 2013.
Dr. Richard M Hill
Damin LT.

Sums of two squares.

Some numbers can be written as a sum of two squares: $1=1^2+0^2$, $2=1^2+1^2$, $4=2^2+0^2$, $5=2^2+1^2$, $8=2^2+2^2$, $9=3^2+0^2$, $10=3^2+1^2$.

Some cannot: e.g. 3, 6, 7. Which integers can be expressed as the sum of two squares: a^2+b^2, $a,b\in\mathbb{Z}$?

We recall the decomposition theorem for the Gaussian integers: $N(1+i)=2$, $N(\pi)=p$ etc...

The question above is equivalent to – which integers n are of the form $n=N(x+iy)=x^2+y^2$?

For instance, if p is a prime s.t. $p\equiv 3 \bmod 4$, then there is no element of $\mathbb{Z}[i]$ with norm 3. $\therefore$ 3 is not a sum of two squares.

Theorem (Two Squares Theorem).

Let n be a positive integer, $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ (p_i are distinct primes). Then the following are equivalent:

① n is a sum of two squares, ② for each prime $p_i\equiv 3 \bmod 4$, the power of a_i is even.

Proof – (① ⇒ ②) Assume $n=x^2+y^2=N(x+iy)=N(\alpha)$ where $\alpha=x+iy$. Factorise α into Gaussian primes: $\alpha=\pi_1\pi_2\cdots\pi_d$. Then $n=N(\alpha)$, and $n=N(\alpha)=N(\pi_1)N(\pi_2)\cdots N(\pi_d)$. Then $N(\pi_i)=\begin{cases}2,\\ p, & \text{where } p\equiv 1 \bmod 4\\ p^2, & \text{where } p\equiv 3 \bmod 4.\end{cases}$ $\therefore$ if $p\equiv 3 \bmod 4$, then power of p in n must be even.

(② ⇒ ①) Define Gaussian integer α_i depending on $p_i^{a_i}$. If $p_i\equiv 1\ (4)$ or $p_i=2$, then $\exists$ a Gaussian prime π_i of norm p_i. Let $\alpha_i=\pi_i^{a_i}$.

$\therefore N(\alpha_i)=p_i$. If $p_i\equiv 3\ (4)$, then a_i is even $\Rightarrow \alpha_i$ is then $\alpha_i=p_i^{a_i/2}\in\mathbb{Z}[i]$. $N(\alpha_i)=p_i^{a_i}$. Let $\alpha=\alpha_1\cdots\alpha_r$.

Then $N(\alpha)=N(\alpha_1)\cdots N(\alpha_r)=p_1^{a_1}\cdots p_r^{a_r}=n$ $\therefore$ n is a sum of two squares.

The proof shows how to write n as a sum of two squares.

Ex Write 585 as a sum of two squares, if possible.

Soln. $585=5\times 3^2\times 13$. Since power of 3 is even, 585 is a sum of two squares. $5=2^2+1^2=(2+i)(2-i)$, $13=3^2+2^2=(3+2i)(3-2i)$.

Let $\alpha=(2+i)3(3+2i)$ or $(2-i)3(3+2i)$ or $(2+i)3(3-2i)$ or $(2-i)3(3-2i)$. Each of these elements α has norm $5\times 9\times 13=585$.

We have $\alpha=12+21i,\ 12-21i,\ 24-3i,\ 24+3i$. Thus, $585=21^2+12^2=24^2+3^2$.

Chapter 6.
CONTINUED FRACTIONS and PELL'S EQUATION.

Definition A finite continued fraction is $a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cdots+\cfrac{1}{a_n}}}$ where $a_i\in\mathbb{Z}$ and $a_i>0$ for $i=1,\dots,n$. We write this as $[a_0,a_1,\dots,a_n]$.

Ex Find $[1,2,3,2]$ in simplified form.

Soln. $[1,2,3,2]=1+\cfrac{1}{2+\cfrac{1}{3+\frac{1}{2}}}=1+\cfrac{1}{2+\frac{1}{(7/2)}}=1+\cfrac{1}{2+\frac{2}{7}}=1+\frac{1}{16/7}=1+\frac{7}{16}=\frac{23}{16}$.

Obviously, every finite continued fraction is a rational number. The converse is also true: every rational number is a finite continued fraction.

Ex Express $\frac{89}{35}$ as a continued fraction.

Soln. Go through Euclidean algorithm with 89, 35. $89=2\cdot 35+19$, $35=1\cdot 19+16$, $19=1\cdot 16+3$, $16=5\cdot 3+1$, $3=3\cdot 1+0$.

We rewrite this as $\frac{89}{35}=2+\frac{19}{35}$, $\frac{35}{19}=1+\frac{16}{19}$, $\frac{19}{16}=1+\frac{3}{16}$, $\frac{16}{3}=5+\frac{1}{3}$. $\therefore \frac{89}{35}=2+\frac{19}{35}=2+\left(\frac{35}{19}\right)^{-1}=2+\left(1+\frac{16}{19}\right)^{-1}=2+\left(1+\left(1+\frac{3}{16}\right)^{-1}\right)^{-1}$

$\therefore \frac{89}{35}=2+[1+(1+[5+\frac{1}{3}]^{-1})^{-1}]^{-1}=2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{5+\frac{1}{3}}}}=[2,1,1,5,3]$.

Note: We can perform these more quickly by noting that $[2,1,1,5,3]$ are the coefficients in the Euclidean algorithm process.

$\boxed{\text{Ex}}$ Express $\frac{102}{47}$ as a continued fraction.

soln. $102 = 2\times 47 + 8$, $47 = 5\times 8 + 7$, $8 = 1\times 7 + 1$, $7 = 7\times 1 + 0 \Rightarrow \frac{102}{47} = [2,5,1,7]$ //.

Suppose we have a sequence of integers $a_0, a_1, a_2, \ldots$ with $a_i > 0$ for all $i > 0$. For every n, we have a finite continued fraction $x_n = [a_0, a_1, \cdots, a_n]$.

The infinite continued fraction $[a_0, a_1, a_2, \ldots]$ is the limit of x_n as $n \to \infty$.

We will prove that this limit exists. $x_0 = [a_0] = a_0$, $x_1 = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$. $x_2 = [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\left(\frac{a_1 a_2 + 1}{a_2}\right)} = a_0 + \frac{a_2}{a_1 a_2 + 1}$.

$x_2 = \frac{a_2(a_0 a_1 + 1) + a_0}{a_1 a_2 + 1}$. Define two sequences of integers h_n, k_n by $h_0 = a_0$, $h_1 = a_0 a_1 + 1$, ..., $h_n = a_n h_{n-1} + h_{n-2}$ $(n \geq 2)$.

$k_0 = 1$, $k_1 = a_1$, $k_n = a_n k_{n-1} + k_{n-2}$.

$\boxed{\text{Lemma}}$ $[a_0, \cdots, a_n] = \frac{h_n}{k_n}$. More generally for $\alpha \in \mathbb{R}$, $[a_0, \cdots, a_n, \alpha] = \frac{h_n \alpha + h_{n-1}}{k_n \alpha + k_{n-1}}$ where $[a_0, \cdots, a_n, \alpha] = a_0 + \frac{1}{a_1 + \cdots + \frac{1}{a_n + \frac{1}{\alpha}}}$.

Proof – By induction on n. We can check this for $n=0, n=1$. Assume true for $n-1$. Then $[a_0, \cdots, a_n, \alpha] = [a_0, \cdots, a_n + \frac{1}{\alpha}] = \frac{h_{n-1}(a_n + \frac{1}{\alpha}) + h_{n-2}}{k_{n-1}(a_n + \frac{1}{\alpha}) + k_{n-2}}$

(true by inductive hypothesis) $= \frac{h_{n-1} a_n \alpha + h_{n-1} + h_{n-2}\alpha}{k_{n-1} a_n \alpha + k_{n-1} + k_{n-2}\alpha} = \frac{(a_n h_{n-1} + h_{n-2})\alpha + h_{n-1}}{(a_n k_{n-1} + k_{n-2})\alpha + k_{n-1}} = \frac{h_n \alpha + h_{n-1}}{k_n \alpha + k_{n-1}}$ (by definition) // q.e.d.

Take limits: $[a_0, \ldots, a_n] = \lim_{\alpha \to \infty} [a_0, \ldots, a_n + \frac{1}{\alpha}] = \lim_{\alpha \to \infty} \frac{h_n \alpha + h_{n-1}}{k_n \alpha + k_{n-1}} = \frac{h_n}{k_n}$ // q.e.d.

$\boxed{\text{Lemma}}$ h_n, k_n are coprime, and $h_{n+1} k_n - h_n k_{n+1} = (-1)^n$.

Proof – The formula implies that h_n, k_n are coprime, if it holds. We just prove the formula: we can check this for $n = 0, 1$. Assume true for $n-1$.

then $h_{n+1} k_n - h_n k_{n+1} = (a_{n+1} h_n + h_{n-1}) k_n - h_n (a_{n+1} k_n + k_{n-1}) = h_{n-1} k_n - h_n k_{n-1} = (-1)[h_n k_{n-1} - h_{n-1} k_n] = (-1)^{n-1} \cdot (-1) = (-1)^n$ // q.e.d.

$\boxed{\text{Theorem}}$ The numbers $x_n = \frac{h_n}{k_n} = [a_0, \ldots, a_n]$ converge to a limit $x \in \mathbb{R}$. The limit x lies between x_n and x_{n+1}; and $|x - x_n| \leq \frac{1}{k_n k_{n+1}} < \frac{1}{k_n^2}$.

Pell's equation: Let $d \in \mathbb{N}$, not a square. Pell's equation is $x^2 - dy^2 = 1$. Solution corresponds to invertible elements in $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}$.

The method for solving Pell's equation involves continued fractions: $(\frac{x}{y})^2 - d = \frac{1}{y^2}$, so $\frac{x}{y}$ is approximately $\sqrt{d}$.

To find rational numbers close to $\sqrt{d}$, we write $\sqrt{d}$ as an infinite continued fraction: $\sqrt{d} = [a_0, a_1, \cdots]$. The solutions will be (h_n, k_n) i.e. $x = h_n$, $y = k_n$.

Proof – (of Thm). $x_{n+1} - x_n = \frac{h_{n+1}}{k_{n+1}} - \frac{k_{n+1}}{k_n} = \frac{h_{n+1} k_n - h_n k_{n+1}}{k_n k_{n+1}} = \frac{(-1)^n}{k_n k_{n+1}}$ by the Lemma. Then $x_n = x_0 + (x_1 - x_0) + (x_2 - x_1) + \cdots + (x_n - x_{n+1})$

$\Rightarrow x_n = x_0 + \frac{1}{k_0 k_1} + \frac{1}{k_1 k_2} + \cdots \frac{1}{k_{n-1} k_n}$, so $\lim_{n\to\infty} x_n = x_0 + \sum_{n=0}^{\infty} \frac{(-1)^n}{k_n k_{n+1}}$. This converges by alternating series test. $\therefore \lim_{n\to\infty} x_n$ also converges // q.e.d.

Also by alternating series test, $\sum_{n=0}^{\infty} \frac{(-1)^n}{k_n k_{n+1}}$ is between $\sum_{n=0}^{N} \frac{(-1)^n}{k_n k_{n+1}}$ and $\sum_{n=0}^{N+1} \frac{(-1)^n}{k_n k_{n+1}}$. (Equivalently, $x \in (x_n, x_{n+1})$.)

$\therefore |x - x_n| < |x_{n+1} - x_n| = \frac{1}{k_n k_{n+1}} < \frac{1}{k_n^2}$ // q.e.d.

5 March 2013
Dr. Richard HILL
Darwin LT.

$\boxed{\text{Ex}}$ Let $x = [1,2,1,2,1,2,\ldots]$. Calculate x.

Soln. We can write $x = 1 + \frac{1}{2 + \frac{1}{x}}$ since the pattern just repeats. Then just solving for x, we get $x = 1 + \frac{1}{\frac{2x+1}{x}} = 1 + \frac{x}{2x+1} = \frac{2x+1+x}{2x+1}$

$\Rightarrow x(2x+1) = 3x+1 \Rightarrow 2x^2 + x - 3x - 1 = 0 \Rightarrow 2x^2 - 2x - 1 = 0 \Rightarrow x = \frac{2 \pm \sqrt{4+8}}{4} = \frac{1 \pm \sqrt{3}}{2}$. Since x is clearly positive, we chose the positive solution, $x = \frac{1+\sqrt{3}}{2}$.

Remark: If we have any finite periodic continued fraction, then it is always of the form $a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$, $d \in \mathbb{Z}$. We can calculate them by the same method.

$\boxed{\text{Proposition}}$ If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then $\exists$ a sequence of integers $a_0, a_1, a_2, \cdots \in \mathbb{Z}$, with $a_n > 0$ for $n > 0$, s.t. $\alpha = [a_0, a_1, a_2, \ldots]$.

Proof – We define sequences $\alpha_n \in \mathbb{R}$, $a_n \in \mathbb{Z}$ s.t. $\alpha_0 = \alpha$, $a_0 = \lfloor \alpha \rfloor$, $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$, $a_{n+1} = \lfloor \alpha_{n+1} \rfloor$. Note that $0 < \alpha_n - a_n < 1$ and so $\alpha_{n+1} > 1 \Rightarrow a_{n+1} = \lfloor \alpha_{n+1} \rfloor \geq 1$.

Now write $\alpha = \alpha_0 = a_0 + (\alpha_0 - a_0) = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{a_1 + (\alpha_1 - a_1)} = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}$ etc.

In general, $\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$ for any n. We want to prove that $[a_0, a_1, \ldots, a_n] \to \alpha$ as $n \to \infty$. It suffices to show that α lies between $[a_0, \ldots, a_{n-1}]$ and $[a_0, \ldots, a_n]$.

$0 < a_n < \alpha_n \therefore 0 < \frac{1}{\alpha_n} < \frac{1}{a_n} \therefore a_{n-1} < a_{n-1} + \frac{1}{\alpha_n} < a_{n-1} + \frac{1}{a_n}$ where $a_{n-1} = a_0 + \frac{1}{a_1 + \frac{1}{\ddots a_{n-2} + \frac{1}{a_{n-1}}}}$, $a_n = a_0 + \frac{1}{a_1 + \frac{1}{\ddots \frac{1}{a_{n-1} + \frac{1}{a_n}}}}$

and clearly $a_{n-1} + \frac{1}{\alpha_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ddots \frac{1}{a_{n-1} + \frac{1}{\alpha_n}}}}$ is between them. But it is equal to α, so we have that $\alpha \in ([a_0, \ldots, a_{n-1}], [a_0, \ldots, a_{n-1}, a_n])$.

The proof of this gives us an algorithm to approach this: Finding the continued fraction expansion of an irrational number α.

1. Define $a_n = \lfloor \alpha_n \rfloor$, $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$, $\alpha_0 = \alpha$ and $a_0 = \lfloor \alpha \rfloor$.
2. Find the terms of the sequence a_n (not always easy/possible. Compute as many as needed if a pattern seems to be emerging).
3. Then $\alpha = [a_0, a_1, a_2, \ldots]$

$\boxed{\text{Ex}}$ Find the continued fraction of $\alpha = \sqrt{2}$.

Soln. We write $\alpha_0 = \sqrt{2}$, $a_0 = \lfloor \sqrt{2} \rfloor = 1$ and define $a_n = \lfloor \alpha_n \rfloor$, $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$. Then $\alpha_1 = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} = \sqrt{2} + 1 \Rightarrow a_1 = \lfloor \sqrt{2} + 1 \rfloor = 2$.

$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = \alpha_1 \Rightarrow a_2 = 2 = a_1$. Continuing in this way, we get $a_3 = 2$, $a_n = 2 \ \forall n \geq 1$, so $\sqrt{2} = [1,2,2,2,\ldots] = [1,\overline{2}]$ //

Further Exercise: Find a continued fraction expression for $2^{1/3}$.

<u>Pell's Equation</u>: $x^2-dy^2=1$.

let $d=2$. Then $x^2-2y^2=1 \Rightarrow (\frac{x}{y})^2-2=\frac{1}{y^2}$. Then if $x^2-2y^2=1$, we get by dividing by y^2: $(\frac{x}{y})^2-2=\frac{1}{y^2}$. If y is very big, $\frac{1}{y^2}$ is negigible so $\frac{x}{y}\approx\sqrt{2}$. But we found $\frac{h_n}{k_n}\in\mathbb{Q}$ s.t. $\frac{h_n}{k_n}\to\sqrt{2}$, where $\frac{h_n}{k_n}=[1,2,2,2,\dots]$.

We can now find solutions of Pell's equation, i.e. pairs (x,y) which satisfy $x^2-2y^2=1$.

- $\frac{h_0}{k_0}=[1]=\frac{1}{1}$, $1^2-2\cdot1^2=-1\neq1$, not a solution.
- $\frac{h_1}{k_1}=[1,2]=1+\frac{1}{2}=\frac{3}{2}$. $3^2-2\times2^2=1\Rightarrow(3,2)$ is a solution//
- $\frac{h_2}{k_2}=[1,2,2]=1+\frac{1}{2+\frac{1}{2}}=1+\frac{1}{5/2}=\frac{7}{5}$. $7^2-2\cdot5^2=-1\Rightarrow$ not a solution.
- $\frac{h_3}{k_3}=[1,2,2,2]=1+\frac{1}{2+\frac{1}{2+\frac{1}{2}}}=1+\frac{1}{2+(5/2)^{-1}}=\frac{17}{12}$. $17^2-2\times12^2=289-288=1\Rightarrow$ so $(17,12)$ is a solution//

11 March 2013.
Dr. Richard HILL.
Damin LT.

<u>Best approximations.</u>

let α be an irrational real number. we can write α as an infinite continued fraction: $\alpha=[a_0,a_1,a_2,\dots]$ $a_n\in\mathbb{Z}$, $a_n>0$ if $n>0$.

consider $\frac{h_n}{k_n}=[a_0,\dots,a_n]$: this is the "$n^{th}$ convergent" to α; $\frac{h_n}{k_n}\to\alpha$. $|\alpha-\frac{h_n}{k_n}|<\frac{1}{k_n^2}$. α is between $\frac{h_n}{k_n}$ and $\frac{h_{n+1}}{k_{n+1}}$.

$h_0=a_0$, $h_1=a_1a_0+1$, $\dots$, $h_n=a_nh_{n-1}+h_{n-2}$. $k_0=1$, $k_1=a_1$, $k_n=a_nk_{n-1}+k_{n-2}$. k_n is an increasing sequence of positive integers.

$\text{hcf}(h_n,k_n)=1$: $h_{n+1}k_n-h_nk_{n+1}=(-1)^n$.

Definition A rational number $\frac{a}{b}$ is called a <u>best approximation to α</u> if for all rational numbers $\frac{c}{d}$ if $|\alpha-\frac{c}{d}|<|\alpha-\frac{a}{b}|\Rightarrow d>b$.

For instance, 3 and $\frac{22}{7}$ are best approximations to π.

Theorem $\forall n$, $\frac{h_n}{k_n}$ is a best approximation to α.

Lemma suppose $\frac{a}{b}\in\mathbb{Q}$, $\frac{a}{b}\neq\frac{h_n}{k_n}$, $0<b<k_{n+1}$. then $|b\alpha-a|>|k_n\alpha-h_n|$.

Proof – consider the simultaneous equations $h_nx+h_{n+1}y=a$; $k_nx+k_{n+1}y=b$. since $\det\begin{pmatrix}h_n & h_{n+1}\\ k_n & k_{n+1}\end{pmatrix}=\pm1\neq0$, unique solution exists:

i.e. $\exists(x,y)$, $x,y\in\mathbb{Z}$ that solves this system. Neither x nor y is 0. $\because\frac{a}{b}\neq\frac{h_n}{k_n}$, $\frac{a}{b}\neq\frac{h_{n+1}}{k_{n+1}}$.

Also, x and y have opposite signs. this follows from second equation, because $0<b<k_{n+1}$. $\alpha-\frac{h_n}{k_n}$ and $\alpha-\frac{h_{n+1}}{k_{n+1}}$ have opposite signs ($\because\alpha$ is between them). $|b\alpha-a|=|(k_nx+k_{n+1}y)\alpha-(h_nx+h_{n+1})y|=|x(k_n\alpha-h_n)+y(k_{n+1}\alpha-h_{n+1})|$. By parities, $|b\alpha-a|=|x||k_n\alpha-h_n|+|y||k_{n+1}\alpha-h_{n+1}|$

$\because x(k_n\alpha-h_n)$ and $y(k_{n+1}\alpha-h_{n+1})$ have the same sign $\Rightarrow|b\alpha-a|>|k_n\alpha-h_n|$.

(Thm).
Proof – chose $\frac{a}{b}$ with $0<b\leq k_n$, if $\frac{a}{b}\neq\frac{h_n}{k_n}$, then NTP: $|\alpha-\frac{a}{b}|>|\alpha-\frac{h_n}{k_n}|$. By the Lemma, $|b\alpha-a|>|k_n\alpha-h_n|$. Then

$|\alpha-\frac{a}{b}|>\frac{k_n}{b}|\alpha-\frac{h_n}{k_n}|\geq|\alpha-\frac{h_n}{k_n}|$// q.e.d.

Proposition suppose $\frac{a}{b}\in\mathbb{Q}$ with $|\alpha-\frac{a}{b}|<\frac{1}{2b^2}$. then $\frac{a}{b}$ is one of the convergents $\frac{h_n}{k_n}$.

Proof - Assume $\frac{a}{b}$ is not one of the convergents. The denominators k_n are increasing so $\exists n$ s.t. $k_n\leq b<k_{n+1}$; and also $\frac{a}{b}\neq\frac{h_n}{k_n}$.

$\therefore$ By the lemma, $|b\alpha-a|>|k_n\alpha-h_n|$. $\therefore|\alpha-\frac{h_n}{k_n}|<\frac{1}{k_n}|b\alpha-a|<\frac{1}{2bk_n}$. $\frac{a}{b}\neq\frac{h_n}{k_n}\Rightarrow|\frac{a}{b}-\frac{h_n}{k_n}|\geq\frac{1}{bk_n}$

$\frac{1}{bk_n}\leq|\frac{a}{b}-\frac{h_n}{k_n}|=|(\frac{a}{b}-\alpha)+(\alpha-\frac{h_n}{k_n})|\leq|\frac{a}{b}-\alpha|+|\alpha-\frac{h_n}{k_n}|<\frac{1}{2b^2}+\frac{1}{2bk_n}\leq\frac{1}{bk_n}$. $\therefore\frac{1}{bk_n}<\frac{1}{bk_n}\Rightarrow$ contradiction// q.e.d.

<u>Pell's equation.</u>

12 March 2013.
Dr. Richard HILL
Damin LT.

Let d be a positive integer, non-square. Pell's equation is $x^2-dy=1$. Let $\mathbb{Z}[\sqrt{d}]=\{x+y\sqrt{d}: x,y\in\mathbb{Z}\}$, $\mathbb{Z}[\sqrt{d}]$ is a ring (closed under $+,\times,-$).

We define $N(x+y\sqrt{d})=x^2-dy^2$. Finding solutions to Pell's equation is equivalent to finding elements of norm 1 in $\mathbb{Z}[\sqrt{d}]$.

Lemma If $\alpha,\beta\in\mathbb{Z}[\sqrt{d}]$ then $N(\alpha\beta)=N(\alpha)N(\beta)$.

Proof - suppose $\alpha=a+b\sqrt{d}$, $\beta=x+y\sqrt{d}$ $\therefore\alpha\beta=(ax+byd)+\sqrt{d}(ay+bx)$. $N(\alpha\beta)=(ax+byd)^2-d(ay+bx)^2$. $N(\alpha)=a^2-db^2$, $N(\beta)=x^2-dy^2$.

$N(\alpha)N(\beta)=a^2x^2-da^2y^2-db^2x^2+d^2b^2y^2$. $N(\alpha\beta)=a^2x^2+2abxyd+b^2y^2d^2-da^2y^2-2dabxy-db^2x^2$ $\therefore N(\alpha\beta)=N(\alpha)N(\beta)$// q.e.d.

Corollary The elements of $\mathbb{Z}[\sqrt{d}]$ with norm 1 form a group with operation $\times$.

Proof - suppose α,β have norm 1, $N(\alpha\beta)=N(\alpha)N(\beta)=1\times1=1$. $\therefore$ elements of norm 1 are closed under $\times$. If $\alpha=x+y\sqrt{d}$, $N(\alpha)=1$.

$\therefore(x+y\sqrt{d})(x-y\sqrt{d})=1$ $\therefore\frac{1}{\alpha}=x-y\sqrt{d}$. this also has norm 1// q.e.d.

$x^2-dy^2=1$: the solutions $(1,0)$ and $(-1,0)$ are called the trivial solutions. The <u>fundamental solution</u> is the smallest non-trivial solution with $x,y>0$.

Corollary let (x_0,y_0) be the fundamental solution to Pell's equation. Then every element of $\mathbb{Z}[\sqrt{d}]$ with norm 1 has the form $\pm(x_0+y_0\sqrt{d})^n$, $n\in\mathbb{Z}$.

e.g. $d=3$, $x^2-3y^2=1$. $(2,1)$ is the fundamental solution: $2+\sqrt{3}$ has norm 1. $(2+\sqrt{3})^3=8+3\times4\times\sqrt{3}+3\times2\times3+3\sqrt{3}=26+15\sqrt{3}$ has norm 1.

$\therefore(26,15)$ is another solution to Pell's equation.

Proof - let $\alpha=x_0+y_0\sqrt{d}$. Then α is the smallest element of norm 1, which is >1. let β be any element of norm 1 ($\beta>0$). For some $n\in\mathbb{Z}$,

$\alpha^n\leq\beta\leq\alpha^{n+1}$ $\therefore1\leq\frac{\beta}{\alpha^n}<\alpha\Rightarrow\frac{\beta}{\alpha^n}$ has norm 1 $\therefore\frac{\beta}{\alpha^n}=1$ $\therefore\beta=\alpha^n$. If $\beta<0$, do same thing with $-\beta$.

7701-16.

$\boxed{\text{Theorem}}$ Let α be an irrational number. Suppose $\frac{a}{b}$ is a rational number with $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$. Then $\frac{a}{b} = [a_0, a_1, \dots, a_n]$ where $\alpha = [a_0, a_1, a_2, \dots]$

$\boxed{\text{Corollary}}$ Suppose x, y is a solution to Pell's equation with $x, y > 0$. Then $\frac{x}{y} = [a_0, \dots, a_n]$ for some n, where $\sqrt{d} = [a_0, a_1, a_2, \dots]$

Proof – $x^2 - dy^2 = 1 \Rightarrow (x + y\sqrt{d})(x - y\sqrt{d}) = 1$. $\therefore x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}}$ $\therefore \frac{x}{y} - \sqrt{d} = \frac{1}{xy + y^2\sqrt{d}}$ $\therefore |\frac{x}{y} - \sqrt{d}| < \frac{1}{2y^2}$

By the theorem, $\frac{x}{y} = [a_0, \dots, a_n]$ for some n. // q.e.d.

To solve Pell's Equation:

- Write $\sqrt{d}$ as a continued fraction
- Calculate a few convergents. Check to see if (h_0, k_0) is a solution to Pell's equation
- Let (h, k) be the first solution that we find. Then (h, k) is the fundamental solution.
- If (x, y) is any solution, $x + y\sqrt{d} = \pm(h + k\sqrt{d})^n$ for some n.

$\boxed{\text{Ex}}$ Solve $x^2 - 7y^2 = 1$.

Soln. Write $\sqrt{7}$ as a continued fraction. $a_0 = [\sqrt{7}] = 2$. $\alpha_0 = \sqrt{7}$, $\alpha_1 = \frac{1}{\sqrt{7} - a_0} = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7}+2}{3}$ $\therefore a_1 = [\alpha_1] = 1$. $\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\frac{\sqrt{7}+2}{3} - 1} = \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}$. $a_2 = 1$.

$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{\frac{\sqrt{7}+1}{2} - 1} = \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$, $a_3 = \lfloor \frac{\sqrt{7}+1}{3} \rfloor = 1$. $\alpha_4 = \frac{1}{(\frac{\sqrt{7}-2}{3})} = \frac{3(\sqrt{7}+2)}{3} = \sqrt{7} + 2$. $a_4 = 4$. $\alpha_5 = \frac{1}{(\sqrt{7}+2) - 4} = \frac{1}{\sqrt{7} - 2} = \alpha_1$, $a_5 = a_1$. etc.

$\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \dots\dots] = [2, \overline{1, 1, 1, 4}]$. The smallest solution with $x > 0$, $y > 0$ is called the fundamental solution.

18 March 2013.
Dr. RM Hill
Domin 4.

All solutions are of form (x, y), where $x + y\sqrt{7} = \pm(x_0 + \sqrt{7}\, y_0)^n$, $n \in \mathbb{Z}$.

To find fundamental solution, check (h_n, k_n). $\frac{h_0}{k_0} = [2] = 2 = \frac{2}{1}$. check: $2^2 - 7 \cdot 1^2 \neq 1$, so not a solution. $\frac{h_1}{k_1} = [2, 1] = 2 + \frac{1}{1} = \frac{3}{1}$. Check: $3^2 - 7 \cdot 1^2 \neq 1$, not.

$\frac{h_2}{k_2} = [2, 1, 1] = 2 + \frac{1}{1 + \frac{1}{1}} = 2 + \frac{1}{2} = \frac{5}{2}$. check: $5^2 - 7 \cdot 2^2 = -3 \neq 1$. $\frac{h_3}{k_3} = [2, 1, 1, 1] = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = 2 + \frac{2}{3} = \frac{8}{3}$. Then we check: $8^2 - 7 \cdot 3^2 = 64 - 63 = 1$.

Hence, $(8, 3)$ is fundamental solution. Any other solution (x, y) obeys $x + y\sqrt{7} = \pm(8 + 3\sqrt{7})^n$.

END OF SYLLABUS.