

## Summary of week 1 lectures

**Notation.** For two integers  $a, b \in \mathbb{Z}$ , we'll say that  $a$  divides  $b$  or  $a$  is a factor of  $b$  or  $b$  is a multiple of  $a$  if there is an integer  $c$  such that  $b = ac$ . This is written  $a|b$ .

An integer  $p \geq 2$  is called a *prime number* if the only factors of  $p$  are  $\pm 1$  and  $\pm p$ . An integer  $n \geq 2$  which is not prime is called *composite*.

The largest integer which is a factor of both  $a$  and  $b$  is called the *highest common factor* of  $a$  and  $b$ , and is written  $\text{hcf}(a, b)$ . If their highest common factor is 1, then we say that  $a$  and  $b$  are *coprime*.

Two integers  $a, b$  are *congruent modulo  $n$*  if  $a - b$  is a multiple of  $n$ . This is written  $a \equiv b \pmod{n}$ . We write  $\mathbb{Z}/n = \{0, 1, 2, \dots, n-1\}$  for the integers modulo  $n$ , i.e. the usual integers with  $a$  and  $b$  regarded as equal if  $a \equiv b \pmod{n}$ . We have operations  $+$ ,  $-$  and  $\times$  on  $\mathbb{Z}/n$  satisfying the usual rules, so  $\mathbb{Z}/n$  is a *ring*.

If  $p$  is a prime number then all non-zero elements of  $\mathbb{Z}/p$  are invertible, so  $\mathbb{Z}/p$  is a field. We usually write  $\mathbb{F}_p$  instead of  $\mathbb{Z}/p$  for this field.

An element  $a \in \mathbb{Z}/n$  is *invertible modulo  $n$*  if there is an element  $b \in \mathbb{Z}/n$  such that  $ab \equiv 1 \pmod{n}$ . The set of invertible elements in  $\mathbb{Z}/n$  is written  $(\mathbb{Z}/n)^\times$ . This is a group with the operation of multiplication.

**Lemma (Bezout's Lemma).** Given  $a, b \in \mathbb{Z}$  not both zero, there exist  $h, k \in \mathbb{Z}$  such that  $ha + kb = \text{hcf}(a, b)$ .

**Proposition.** An element  $a \in \mathbb{Z}/n$  is invertible modulo  $n$  if and only if  $a$  is coprime to  $n$ .

**Theorem (Chinese remainder theorem).** Let  $n, m$  be coprime. Given  $a \in \mathbb{Z}/n$  and  $b \in \mathbb{Z}/m$  there is a unique  $x \in \mathbb{Z}/nm$  such that  $x \equiv a \pmod{n}$  and  $x \equiv b \pmod{m}$ .

**Theorem (Fermat's little theorem).** Let  $p$  be a prime number and let  $a \in \mathbb{F}_p^\times$ . Then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Method.** Euclid's algorithm gives us a way of finding integers  $h, k$  such that  $ha + kb = \text{hcf}(a, b)$ .

**Method (Finding  $a^{-1} \pmod{n}$ ).** Assume  $a$  and  $n$  are coprime. By Euclid's algorithm we can find integers  $h, k$  such that  $ha + kn = 1$ . Then we reduce this modulo  $n$  to give  $ha \equiv 1 \pmod{n}$ . Therefore  $h$  is the inverse of  $a$  modulo  $n$ .

**Method (Solving  $ax \equiv b \pmod{n}$ ).** There are several cases.

1. If  $a$  is coprime to  $n$ , then we find the inverse of  $a$  modulo  $n$ . Then we have  $x \equiv a^{-1}b \pmod{n}$ .
2. If  $a$  is a factor of  $n$  but  $a$  is not a factor of  $b$ , then there are no solutions.
3. If  $a$  is a factor of both  $n$  and  $b$ , then the solution is  $x \equiv b/a \pmod{n/a}$ .

**Method (Solving simultaneous congruences  $x \equiv a \pmod{n}$ ,  $x \equiv b \pmod{m}$ , where  $n$  and  $m$  are coprime).** To solve these, we first find integers  $h, k$  such that  $hn + km = 1$ . Then the solution is  $x \equiv hnb + kma \pmod{nm}$ .

**Method (Solving  $x^a \equiv b \pmod{p}$ , where  $a$  is coprime to  $p-1$ ).** To solve this, first find the inverse  $a^{-1}$  of  $a$  modulo  $p-1$ . Then raise both sides of the equation to the power  $a^{-1}$ . We get the solution  $x \equiv b^{a^{-1}} \pmod{p}$ .

## Summary of week 2 lectures

**Theorem** (Uniqueness of factorization of integers). *For any positive integer  $n$  there is a factorization  $n = p_1 \cdots p_r$  with each  $p_i$  prime. This factorization is unique up to reordering the primes  $p_1, \dots, p_r$ .*

**Theorem.** *There are infinitely many prime numbers.*

*Notation.* The Euler totient function  $\varphi(n)$  is defined to be the number of invertible elements in  $\mathbb{Z}/n$ , i.e. the order of the group  $(\mathbb{Z}/n)^\times$ .

**Theorem** (Euler). *If  $a$  is invertible modulo  $n$  then  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .*

**Theorem.** *If  $n$  and  $m$  are coprime then there is an isomorphism of groups  $(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$ .*

**Corollary.** *If  $n$  and  $m$  are coprime then  $\varphi(nm) = \varphi(n)\varphi(m)$ .*

**Lemma.** *If  $p$  is prime and  $a \geq 1$  then  $\varphi(p^a) = (p-1)p^{a-1}$ .*

**Corollary.** *Let  $n = p_1^{a_1} \cdots p_r^{a_r}$  with  $p_1, \dots, p_r$  distinct primes. Then  $\varphi(n) = (p_1-1)p_1^{a_1-1} \cdots (p_r-1)p_r^{a_r-1}$ .*

**Method** (Eratosthenes' sieve). If a positive integer  $n$  is composite, then it is divisible by some prime  $p \leq \sqrt{n}$ . Therefore, to find out whether  $n$  is prime or not, we only need to find out whether it is divisible by one of the primes less than  $\sqrt{n}$ .

**Method** (Solving  $x^a \equiv b \pmod{n}$ ). Suppose  $a$  is coprime to  $\varphi(n)$  and  $b$  is coprime to  $n$ . We solve the congruence as follows:

1. Factorize  $n$  into primes and hence calculate  $\varphi(n)$ .
2. Find the inverse  $a^{-1}$  of  $a$  modulo  $\varphi(n)$ .
3. Raise both sides of the equation to the power  $a^{-1}$ . This gives the solution  $x \equiv b^{a^{-1}} \pmod{n}$ .

*Notation.* An element  $a \in \mathbb{F}_p^\times$  is called a *primitive root modulo  $p$*  if  $a$  generates the multiplicative group  $\mathbb{F}_p^\times$ , i.e. if every element of  $\mathbb{F}_p^\times$  is a power of  $a$ .

**Method** (Testing for primitive roots). Let  $p$  be a prime number and  $a \in \mathbb{F}_p^\times$ . To find out whether  $a$  is a primitive root modulo  $p$ :

1. Find the primes  $q$  which divide  $p-1$ .
2. For each such  $q$ , calculate  $a^{(p-1)/q}$  modulo  $p$ . If NONE of these numbers are 1 modulo  $p$  then  $a$  is a primitive root.

## Summary of week 3 lectures

**Proposition.** For any positive integer  $n$ ,

$$\sum_{d|n} \varphi(d) = n.$$

**Theorem (Gauss).** For every prime number  $p$ , there exists a primitive root modulo  $p$ . More precisely there are  $\varphi(p-1)$  of them.

**Definition.** Let  $p$  be an odd prime number and  $a \in \mathbb{F}_p^\times$  coprime to  $p$ . We call  $a$  a *quadratic residue modulo  $p$*  if the congruence  $x^2 \equiv a \pmod{p}$  has solutions; otherwise  $a$  is called a *quadratic non-residue*. The quadratic residue symbol  $\left(\frac{a}{p}\right)$  is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

**Theorem (Euler's Criterion).** Let  $p$  be an odd prime number and  $a \in \mathbb{F}_p^\times$ . Then

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

**Corollary.** Let  $p$  be an odd prime number and  $a, b \in \mathbb{F}_p^\times$ . Then

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

**Theorem (Quadratic reciprocity law).** If  $p$  and  $q$  are distinct odd primes then

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

**Theorem (First Nebensatz).** If  $p \equiv 1 \pmod{4}$  then  $\left(\frac{-1}{p}\right) = 1$  and if  $p \equiv -1 \pmod{4}$  then  $\left(\frac{-1}{p}\right) = -1$ .

**Theorem (Second Nebensatz).** If  $p \equiv \pm 1 \pmod{8}$  then  $\left(\frac{2}{p}\right) = 1$  and if  $p \equiv \pm 3 \pmod{8}$  then  $\left(\frac{2}{p}\right) = -1$ .

**Method.** Using the reciprocity law we can determine whether  $a$  is a quadratic residue modulo  $p$  without actually solving  $x^2 \equiv a \pmod{p}$ . This might be hard to solve by hand if the numbers are big.

**Method.** By Euler's criterion and the reciprocity law, we get a fast way of calculating  $a^{(p-1)/2} \pmod{p}$ . It's important to calculate this number if we want to find out whether  $a$  is a primitive root modulo  $p$ .

## Summary of week 4 lectures

**Definition.** Let  $p$  be an odd prime. The Gauss sum  $G(p)$  is defined by

$$G(p) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a, \quad \zeta_p = e^{2\pi i/p}.$$

**Lemma.**  $G(p)^2 = (-1)^{(p-1)/2} p$ .

*Notation.* For a non-zero integer  $n$  and a prime number  $p$ , we define  $v_p(n) = a$ , where  $a$  is the largest power such that  $p^a$  is a factor of  $n$ . We define  $v_p(0) = \infty$ . For a rational number we define  $v_p\left(\frac{n}{m}\right) = v_p(n) - v_p(m)$ . The function  $v_p(x)$  is called the *valuation of  $x$  at  $p$* . The ring

$$\mathbb{Z}_{(p)} = \left\{ \frac{n}{m} : n, m \in \mathbb{Z}, p \nmid m \right\} = \{x \in \mathbb{Q} : v_p(x) \geq 0\}.$$

is called the *local ring at  $p$* . This consists of the rational numbers which can be reduced modulo  $p^n$ .

**Theorem (Hensel's Lemma).** Let  $p$  be a prime number and let  $f \in \mathbb{Z}_{(p)}[X]$  be a polynomial. Suppose there is an  $a_0 \in \mathbb{Z}_{(p)}$  such that

$$f(a_0) \equiv 0 \pmod{p^{2c+1}}, \quad \text{where } c = v_p(f'(a_0)).$$

Define a sequence  $(a_n)$  recursively by  $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$ . Then  $a_n \in \mathbb{Z}_{(p)}$  and

$$f(a_n) \equiv 0 \pmod{p^{2c+2^n}}.$$

## Summary of week 5 lectures

**Proposition.** Let  $p$  be an odd prime and let  $a$  be an integer coprime to  $p$ . If the congruence  $x^2 \equiv a$  has solutions modulo  $p$ , then it has solutions modulo  $p^n$  for every  $n$ .

**Proposition.** Let  $a$  be an odd number. If the congruence  $x^2 \equiv a$  has solutions modulo 8 then it has solutions modulo  $2^n$  for every  $n > 0$ . This is the case if and only if  $a \equiv 1 \pmod{8}$ .

**Method.** To find a solution to a congruence  $f(x) \equiv 0 \pmod{p^N}$ , first find an "approximate solution"  $a_0$ , i.e.  $a_0$  satisfies the conditions of Hensel's Lemma. Define a sequence in  $\mathbb{Z}_{(p)}$  by

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

Then for  $n$  large enough,  $a_n$  is a solution modulo  $p^N$ .

**Method.** To find out for which  $n$ , the congruence

$$x^2 \equiv a \pmod{n}$$

has solutions, we use the following method:

1. We first answer this for numbers  $n$  of the form  $p^b$ , where  $p$  is a prime number. If  $p$  is not a factor of  $2a$ , then Hensel's Lemma tells us the following:

**A solutions exists modulo  $p^b$  iff a solution exists modulo  $p$ .**

We can check whether a solution exists modulo  $p$  by quadratic reciprocity.

2. For the prime  $p = 2$ , Hensel's Lemma gives:

**Assume  $a$  is odd. A solutions exists modulo  $2^b$  for all  $b \geq 3$  iff  $a \equiv 1 \pmod{8}$**

3. We deal with other prime powers by hand.
4. For general  $n$ , the Chinese remainder theorem tells us:

**Suppose  $n = p_1^{b_1} \cdots p_r^{b_r}$ . A solution exists modulo  $n$  iff a solution exists modulo each prime power  $p_i^{b_i}$ .**

## Summary of week 6 lectures

*Notation.* Let  $p$  be a prime number. The set  $\mathbb{Z}_{(p)}$  is the set of rational numbers whose denominator is coprime to  $p$ . This is closed under addition and multiplication, so it is a subring of  $\mathbb{Q}$ . If we have a series  $\sum x_n$  of elements of  $\mathbb{Z}_{(p)}$  then we say that the series converges  $p$ -adically if for every  $a$  there are only finitely many terms  $x_n$  which are non-zero modulo  $p^n$ . This is equivalent to saying that  $v_p(x_n) \rightarrow \infty$ . This means that the series converges in  $\mathbb{Z}/p^a$  for every  $a$ .

**Lemma** (The Power Series Trick). *Let  $f, g$  and  $h$  be power series with coefficients in  $\mathbb{Z}_{(p)}$  and assume  $g$  has zero constant term. Suppose that*

- (i)  $f, g$  and  $h$  converge for sufficiently small real numbers  $x$ , and for such numbers we have  $f(g(x)) = h(x)$ ;
- (ii)  $f, g$  and  $h$  converge  $p$ -adically for  $x \in \mathbb{Z}_{(p)}$ .

*Then for all  $x \in \mathbb{Z}/p^n$  we have  $f(g(x)) \equiv h(x) \pmod{p^n}$ .*

**Lemma.** *For a real number  $x$ , let  $[x]$  be the largest integer which is  $\leq x$ . With this notation we have:*

$$v_p(r!) = [r/p] + [r/p^2] + \dots \leq \frac{r}{p-1}.$$

**Theorem.** *Let  $p$  be a prime at least 3. There is an isomorphism*

$$\log : 1 + p\mathbb{Z}/p^n \rightarrow p\mathbb{Z}/p^n,$$

*defined by*

$$\log(1 + px) = px - \frac{p^2 x^2}{2} + \frac{p^3 x^3}{3} - \dots$$

*The inverse function, called  $\exp : p\mathbb{Z}/p^n \rightarrow 1 + p\mathbb{Z}/p^n$  is defined by*

$$\exp(px) = 1 + px + \frac{p^2 x^2}{2} + \frac{p^3 x^3}{3!} + \dots$$

*These series converge  $p$ -adically.*

**Definition.** *If  $a \in \mathbb{Z}_{(p)}$  and  $a \equiv 1 \pmod{p}$ , then we define  $a^x \pmod{p^n}$  for all  $x \in \mathbb{Z}_{(p)}$  by*

$$a^x \equiv \exp(x \log(a)) \pmod{p^n}.$$

## Summary of week 7 lectures

**Definition.** The *Teichmüller lift* of  $a$  to  $\mathbb{Z}/p^n$  is defined to be  $T(a) = a^{p^{n-1}} \in \mathbb{Z}/p^n$ .

**Theorem.** Let  $p$  be a prime number and let  $a \in (\mathbb{Z}/p^n)^\times$ .

1. For  $r > n - 1$  we have  $a^{p^r} \equiv T(a) \pmod{p^n}$ .
2. The element  $T(a)$  satisfies  $T(a)^{p-1} \equiv 1 \pmod{p^{n-1}}$ .
3.  $T(a)$  only depends on  $a$  modulo  $p$  and  $T(a) \equiv a \pmod{p}$ .
4. The map  $T : \mathbb{F}_p^\times \rightarrow (\mathbb{Z}/p^n)^\times$  is an injective homomorphism.

*Remark.* Another way of saying this, is that the sequence  $a^{p^n}$  converges  $p$ -adically and we have  $T(a) = \lim_{n \rightarrow \infty} a^{p^n}$  (the  $p$ -adic limit).

**Corollary.** Every element of  $(\mathbb{Z}/p^n)^\times$  can be written uniquely in the form  $T(x) \cdot \exp(py)$ , where  $x \in \mathbb{F}_p^\times$  and  $y \in \mathbb{Z}/p^{n-1}$ . In other words we have an isomorphism

$$(\mathbb{Z}/p^n)^\times \cong \mathbb{F}_p^\times \times \mathbb{Z}/p^{n-1}.$$

## Summary of week 8 lectures

**Notation.** An integer  $d$  is called square-free if the only factor of  $d$  which is a square is 1. Let  $d$  be a square-free integer which is not equal to 0 or 1. We define the quadratic ring corresponding to  $d$  by

$$\mathbb{Z}[\alpha] = \{x + y\alpha : x, y \in \mathbb{Z}\}, \quad \alpha = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \pmod{4}, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

The ring  $\mathbb{Z}[\alpha]$  is called a real quadratic ring if  $d > 0$ , and a complex quadratic ring if  $d < 0$ . For an element  $A = x + y\sqrt{d}$ , ( $x, y \in \mathbb{Q}$ ) we define the conjugate and norm of  $A$  by  $\bar{A} = x - y\sqrt{d}$ ,  $N(A) = A\bar{A}$ . We have

$$N(x + y\alpha) = \begin{cases} x^2 - dy^2 & \text{if } d \not\equiv 1 \pmod{4}, \\ x^2 + xy + \frac{1-d}{4}y^2 & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

We always have  $N(A) \in \mathbb{Z}$ ,  $N(\bar{A}) = N(A)$  and  $N(AB) = N(A)N(B)$ .

**Definition.** An element  $U$  in a ring  $R$  is a unit if there is an element  $U^{-1} \in R$  such that  $UU^{-1} = 1$ . An element  $P \in R$  is called irreducible if  $P$  is not a unit and for all factorizations  $P = AB$ , either  $A$  is a unit or  $B$  is a unit.

**Lemma.** An element  $A \in \mathbb{Z}[\alpha]$  is a unit iff  $N(A) = \pm 1$ .

**Proposition.** In the case  $d = -1$  the units in  $\mathbb{Z}[i]$  are  $1, -1, i, -i$ . In the case  $d = -3$  the units are  $1, -1, \alpha, -\alpha, \alpha - 1, 1 - \alpha$ . In all other complex quadratic rings the units are  $\pm 1$ .

**Definition.** A quadratic ring  $\mathbb{Z}[\alpha]$  is said to be norm-Euclidean if for every  $A, B \in \mathbb{Z}[\alpha]$  with  $B \neq 0$ , there exist  $Q, R \in \mathbb{Z}[\alpha]$  such that  $A = QB + R$  and  $|N(R)| < |N(B)|$ .

**Definition.** The ring  $R$  is said to have unique factorization if the following is true:

- every non-zero element  $A \in R$  may be written in the form  $A = UP_1 \cdots P_n$  with  $U$  a unit and  $P_i$  irreducible.
- If  $A = U'Q_1 \cdots Q_m$  is another such factorization then  $n = m$  and the  $Q_i$  may be reordered so that  $Q_i = U_i P_i$  for units  $U_i \in R$ .

**Theorem.** In the cases  $d = -1, -2, -3, -7, -11, 2, 3, 5, 13$  the quadratic ring  $\mathbb{Z}[\alpha]$  is norm-Euclidean.

**Theorem.** If  $\mathbb{Z}[\alpha]$  is norm-Euclidean then  $\mathbb{Z}[\alpha]$  has unique factorization.

**Definition.** Let  $p$  be a prime number and let  $\mathbb{Z}[\alpha]$  be a quadratic ring with unique factorization.

- We say that  $p$  splits in  $\mathbb{Z}[\alpha]$  if  $p = P_1 P_2$  for irreducible elements  $P_1, P_2 \in \mathbb{Z}[\alpha]$ , where  $P_1$  is not a unit multiple of  $P_2$ . The irreducible elements  $P_1$  and  $P_2$  have norm  $\pm p$ .
- We say  $p$  is inert in  $\mathbb{Z}[\alpha]$  if  $p$  is an irreducible element in  $\mathbb{Z}[\alpha]$ .
- We say  $p$  is ramified in  $\mathbb{Z}[\alpha]$  if  $p = UP^2$ , where  $U$  is a unit in  $\mathbb{Z}[\alpha]$  and  $P$  is an irreducible element with norm  $\pm p$ .

**Theorem (The Decomposition Theorem).** Let  $\mathbb{Z}[\alpha]$  be a quadratic ring with unique factorization. Let  $p$  be an odd prime number.

- If  $p|d$  then  $p$  is ramified in  $\mathbb{Z}[\alpha]$ .
- If  $\left(\frac{d}{p}\right) = 1$  then  $p$  splits in  $\mathbb{Z}[\alpha]$ .
- If  $\left(\frac{d}{p}\right) = -1$  then  $p$  is inert in  $\mathbb{Z}[\alpha]$ .

The prime 2 splits in  $\mathbb{Z}[\alpha]$  if  $d \equiv 1 \pmod{8}$ ; 2 is inert if  $d \equiv 5 \pmod{8}$  and in all other cases 2 is ramified.



## Summary of week 9 lectures

1. Pell's equation is the equation  $x^2 - dy^2 = 1$ , where  $d \geq 2$  is a square-free integer. This has the trivial solution  $x = 1, y = 0$ . It also has non-trivial solutions with positive integers  $x, y$ . The smallest non-trivial solution is called the *fundamental solution*.
2. If  $(x, y)$  is a solution to Pell's equation then  $N(x + y\sqrt{d}) = 1$ , so  $x + y\sqrt{d}$  is a unit in the real quadratic ring containing  $\sqrt{d}$ . The other solutions to  $N(A) = 1$  are of the form  $A = \pm(x + y\sqrt{d})^n$ , where  $(x, y)$  is the fundamental solution. This gives us all solutions to Pell's equation in terms of the fundamental solution.
3. Let  $a_0, \dots, a_n \in \mathbb{Z}$  with  $a_i > 0$  for all  $i > 0$ . Then we define the finite continued fraction recursively by

$$[a_0] = a_0, \quad [a_0, a_1, \dots, a_n] = a_0 + \frac{1}{[a_1, \dots, a_n]}.$$

Every rational number can be written as a finite continued fraction

4. Infinite continued fractions are defined by

$$[a_0, a_1, a_2, \dots] = \lim_{n \rightarrow \infty} [a_0, \dots, a_n].$$

These limits always exist.

5. To find the continued fraction expansion of a real irrational number, we define two sequences  $a_n \in \mathbb{Z}$  and  $\alpha_n \in \mathbb{R}$  recursively as follows:

$$\alpha_0 = \alpha, \quad a_n = [\alpha_n], \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}.$$

Then we have

$$\alpha = [a_0, \alpha_1] = [a_0, a_1, \alpha_2] = [a_0, a_1, \dots, a_n, \alpha_{n+1}] = [a_0, a_1, a_2, \dots].$$

6. If  $d$  is a square-free positive integer with  $d \geq 2$ , then the continued fraction expansion of  $\sqrt{d}$  is eventually periodic:

$$\sqrt{d} = [a_0, a_1, \dots, a_n, a_1, \dots, a_n, \dots].$$

If  $(x, y)$  is any solution to Pell's equation with  $x, y > 0$  then  $x/y = [a_0, \dots, a_r]$  for some positive integer  $r$ .