# Strangely Typset Results from Number Theory

Edward Chernysh[†] Dana Berman[‡]

April 1st, 2017

[†]edward.chernysh at mail.mcgill.ca
[‡]dana.berman at mail.mcgill.ca

## Contents

In this text we shall both state and prove various results from elementary number theory. The reader should be aware that this is not meant as a primary reference, nor for self-learning. This text is brief and far from complete, much of the proofs will require preliminary knowledge, especially is mathematical analysis and the theory of groups and fields.

We shall begin by covering the ring of integers, denoted $\mathbb{Z}$, especially the primes. We shall prove Bézout's identity for the greatest-common divisor, Fermat's little theorem and Wilson's characterization of primes. We shall conclude the section with a proof of the Chinese Remainder Theorem.

The subsequent chapter will be devoted to the study of the *group of units* modulo a prime $p$, and the existence of primitive roots $\pmod p$. We shall prove some results regarding field-theory and use these to prove the *primitive root theorem.*

Following this we briefly explore the idea of solving quadratic equation $\pmod p$, and shall establish important criteria, such as Euler's Proposition, linking the Legendre symbol to modular arithmetic. Furthermore, we briefly explain *public-key encryption.*

Finally, we develop a short theory of continued-fractions, and use this theory to derive powerful estimates and study sums of squares in the natural numbers $\mathbb{N}$.

# 1 The Ring of Integers $\mathbb{Z}$

## 1.1 Basic identities

We begin with the establishing of Bézout's identity, which is highly useful in practice:

**Proposition 1.1** (Bézout's Identity)**.** *Let $a, b \in \mathbb{Z}$ be non-zero and denote by $d$ their greatest common-divisor. There exist integers $u, v$ such that*

$$d = ua + vb \tag{1}$$

Proof. We consider the set $\mathfrak{S} := \{ax + by > 0 : x, y \in \mathbb{Z}\}$. Our first claim is that this set $\mathfrak{S}$ is non-empty. To see this, we note that we may take the integer expression $a^2 + b^2 > 0$ (since $a, b \neq 0$) which corresponds to letting $x := a, y := b$. Hence, since $\mathfrak{S}$ is a subset of $\mathbb{N}$ it follows that there is a least element, say,

$$d = ua + vb > 0$$

We claim that $d = \gcd(a, b)$. Certainly, since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ it follows that $\gcd(a, b) \mid d$ by the additive property of divisibility. It remains only to show that $d \mid a, b$. By symmetry, it suffices to show that $d \mid a$. We write

$$a = qd + r, \quad 0 \leq r < d,\, q \in \mathbb{Z}$$

We claim that $r = 0$ whence $d \mid a$. Otherwise, $0 < r < d$ and we write by the above:

$$d > r = a - qd = a - q(ua + vb) = (1 - qu)a + (va)b > 0$$

contradicting that $d$ is the least element of $\mathfrak{S}$.

○

We make the note that this theorem gives us an explicit linear representation of the greatest-common divisor, but does not tell one how to compute this value.The reader should note that the Euclidean algorithm fills this gap, one simply proceeds as usual and "reverse substitutes" remainders until one has an expression in terms of the starting integers $a, b$.

**Lemma 1.2** (Euclid's Generalized Lemma)**.** *Let $n, m \in \mathbb{Z}$ with $n, m \neq 0$. If $\gcd(a, n) = 1$ and $a \mid nm$ then $a \mid m$.*

Proof. Since $\gcd(a, n) = 1$ we may write $1 = ua + vn$ for integers $u, v \neq 0$. Now, this implies in particular that

$$m = uam + vnm$$

clearly, we then have $a \mid m$ by additivity of divisibility.

○

We now turn briefly towards modular arithmetic.

## 1.2 Primes and Fields

**Proposition 1.3.** *Let $p$ be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Proof. The case is clear for $\mathbb{Z}/2\mathbb{Z}$; this is just the trivial field. Let $p \geq 3$ and $x \not\equiv 0 \pmod{p}$. It follows that $\gcd(x, p) = 1$. An application of Bézout yields some expression

$$1 + up + vx$$

passing to the reduction modulo $p$ we recover $1 \equiv vx \pmod{p}$. Hence, $v \not\equiv 0$ and of course it follows that $v = x^{-1} \pmod{p}$.

○

We remark that the converse is true as well. Namely, if $\mathbb{Z}/n\mathbb{Z}$ is a field then $n$ must be prime. To see this, we argue by contrapositive and show that for $n$ not prime the ring $\mathbb{Z}/n\mathbb{Z}$ is not a field. Note that a field $\mathbb{K}$ cannot have zero-divisors. To see this, suppose that $x, y \in \mathbb{K}$ are non-zero and $xy = 0$. Since $x \neq 0$ and $\mathbb{K}$ is a field, we may multiply through by $x^{-1}$ to find that $y = x^{-1} \cdot 0 = 0$; a contradiction.

Now, if $n$ is composite then we may write $n = ab$ for integers $1 < a, b < n$. Clearly, $n \nmid a, b$ and as such $a, b \not\equiv 0 \pmod{n}$. On the other-hand, $ab \equiv n \equiv 0 \pmod{n}$ showing that $\mathbb{Z}/n\mathbb{Z}$ has zero-divisors.

**Proposition 1.4** (Fermat's Little Theorem)**.** *Let $p \in \mathbb{N}$ [1] be a prime, then for all $x \not\equiv 0 \pmod{p}$ one has the identity:*

$$x^{p-1} \equiv 1 \pmod{p} \tag{2}$$

[1] We shall always write $\mathbb{N}$ to denote the set $\{1, 2, \ldots\}$

The reader should not confuse this with Fermat's Last Theorem, which is much more difficult to prove.

PROOF. It is easy to verify the proof for $p = 2$, as we only have $1 \not\equiv 0 \pmod 2$. Let us now assume without harm that $p \geq 3$. Fix now $x \not\equiv 0 \pmod p$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, this $x$ has a multiplicative inverse $x^{-1} \pmod p$. Consider now the mapping:

$$\Gamma : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*, \quad a \mapsto x \cdot a$$

We wish to show that this is a bijection. This is clear from the auxiliary map:

$$\Upsilon : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*, \quad a \mapsto x^{-1} \cdot a$$

It is not at all difficult to see that $\Gamma \circ \Upsilon \equiv \mathbf{1} \equiv \Upsilon \circ \Gamma$, hence establishing that $\Gamma$ is a bijection. Loosely speaking, this tells us that the map $\Gamma$ merely "shuffles" the elements of $(\mathbb{Z}/p\mathbb{Z})^*$, implying that $(\mathbb{Z}/p\mathbb{Z})^* = \Gamma\left((\mathbb{Z}/p\mathbb{Z})^*\right)$. That is, taking the product over all elements in the domain and the image of $\Gamma$ we obtain:

$$(p-1)! \equiv \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^*} a \equiv \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \Gamma(a) \equiv x^{p-1} \cdot (p-1)! \pmod p$$

Since $p$ is a prime, each term in the expansion of $(p-1)!$ is invertible, and successive division yields that $x^{p-1} \equiv 1 \pmod p$ as was required.

○

We now prove Wilson's Theorem:

**Proposition 1.5** (Wilson's Theorem)**.** *Let $p \in \mathbb{N}$. Then $(p-1)! \equiv -1 \pmod p$ if and only if $p$ is prime.*[2]

PROOF. Assume that $p$ is prime. One may verify by direct calculation the claim in the cases $p = 2, 3$, thus we may suppose without harm to the proof that $p \geq 5$ is an odd prime. Note that $(-1)^2 \equiv 1^2 \equiv 1 \pmod p$. We claim these are the only numbers modulo $p$ that are their own inverses under multiplication. Certainly, if $x^2 \equiv 1 \pmod p$ it follows that $x^2 - 1 \equiv 0 \pmod p$ and hence that $p \mid (x+1)(x-1)$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, one of these factors must be zero. Namely, $x \equiv \pm 1 \pmod p$. This shows especially that each element appearing in the enumeration $\{2, 3, \ldots, p-2\}$ has a unique *distinct* inverse appearing in this list. Since this enumeration contains evenly many elements it follows that

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod p$$

since $(p-1) \equiv -1 \pmod p$ the implication follows.

Conversely, suppose that $(p-1)! \equiv -1 \pmod p$ but that $p$ is composite; i.e. there are integers $1 < a, b < p$ such that $p = ab$. Then, it is clear that $p = ab \mid (p-1)!$ implying that $(p-1)! \equiv 0 \not\equiv -1 \pmod p$, which is non-sense.

○

[2]Observe that one may derive Fermat's Little Theorem from Wilson's Theorem.

Now the time has come to briefly consider solving modular systems of equations. Note that we have already established how to solve certain linear equations. Indeed, our proof that $\mathbb{Z}/p\mathbb{Z}$ is a field for a prime $p$ gave a way to construct the multiplicative inverse to a non-zero number in $\mathbb{Z}/p\mathbb{Z}$. More generally, consider the equation

$$ax \equiv b \pmod{n}$$

where $\gcd(a, n) = 1$. The same argument guarantees the existence of a multiplicative inverse $a^{-1}$ modulo $n$ for $a$. Hence, $x \equiv a^{-1}b \pmod{n}$ where $a^{-1}$ may be computed using Bézout as before.

## 1.3 Chinese Remainder Theorem

**Proposition 1.6** (Chinese Remainder Theorem)**.** *Let $n, m \geq 2$ be co-prime integers. There exists an integer solution to the following system of congruences:*

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \tag{3}$$

*for integers $a, b$. Moreover, up to a reduction modulo $nm$ this $x \in \mathbb{Z}$ is unique.*

Proof. We shall argue by construction. Again, since $\gcd(n, m) = 1$ there exists a multiplicative inverse to $n$, say, $n^{-1} \in \mathbb{Z}/m\mathbb{Z}$ and similarly for $m^{-1} \in \mathbb{Z}/n\mathbb{Z}$. We now define the integer (where we assume the representatives are in their "reduced" form)

$$x := amm^{-1} + bnn^{-1}$$

it may be easily verified that this integer $x$ satisfies the system above. To see uniqueness, we suppose that $x, y$ are integer classes that satisfy the system above. Then, $n \mid (x - y)$ and $m \mid (x - y)$. First of all, $(x - y) = \alpha \cdot n$. Since $n, m$ are co-prime it follows that $m \mid \alpha$ and hence we have $(x - y) \equiv 0 \pmod{nm}$.

◯

In the case where this last line was not entirely clear;

## 1.4 The Group of Units Modulo $p$

Given an integer $n \geq 2$ we shall write $\mathbb{Z}_n^*$ to denote the group of units modulo $n$:

$$\mathbb{Z}_n^* = (\mathbb{Z}/n\mathbb{Z})^* = \{1 \leq x \leq n - 1 : \gcd(x, n) = 1\} \tag{4}$$

it is left to the reader to verify that this forms a group under multiplication. The Euler Totient Function is defined by:

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad n \mapsto \#\left(\mathbb{Z}_n^*\right) \tag{5}$$

This section is devoted to the gleaning knowledge from $\mathbb{Z}_p^*$, where $p$ is prime.

It may easily be shown by induction that given a field $\mathbb{K}$ a polynomial $f \in \mathbb{K}[x]$ of degree $d \geq 1$ has at-most $d$ roots in $\mathbb{K}$. What is of greater use is the subsequent lemma:

### 1.4.1 Polynomials modulo $p$

**Lemma 1.7.** *Let $p$ be a prime. The polynomial $f(x) := x^d - 1$ has exactly $d$ roots modulo $p$ where $d \mid p-1$.*

PROOF. We already know the number of roots is $\leq d$. Take $e := \frac{p-1}{d}$ and consider the expression,

$$x^{p-1} - 1 \equiv x^{de} - 1 \equiv \left(x^d\right)^e - 1 = (x^d - 1)\left(x^{d(e-1)} + x^{d(e-2)} + \cdots + 1\right)$$

Now, we know from Fermat's little theorem that this polynomial has exactly $p-1$ roots modulo $p$. Now, the expression on the RHS has no-more than $d(e-1)$ roots. Denote by $\delta$ the number of roots of $x^d - 1$ modulo $p$. Then, $\delta \geq p - 1 - d(e-1) = p - 1 - (de - d) = d$. This proves the lemma.

◯

Let us now consider a group $G$ of finite order. Let $g, h \in G$ have order $n, m$ respectively, but assume that $\gcd(n, m) = 1$. Then $ab$ has order $nm$ in $G$. This is a well known fact from group theory but we give the proof nonetheless. Let $\ell := o_G(gh)$. We know that $\ell \mid nm$ since $(ab)^{nm} = e$. Now, as a result since $n, m$ are co-prime we may write by Euclid's lemma: $\ell = rs$ where $r \mid n$ and $s \mid m$.[3] Let us now write:

$$e = (ab)^\ell = (ab)^{rs} \implies [(ab)^{rs}]^{\frac{n}{r}} = e$$

Hence, $e = a^{ns}b^{ns} = b^{ns}$ whence $b^{ns} \mid m$ and $s \mid m$. Similarly, we write

$$e = [(ab)^{rs}]^{\frac{m}{s}} = a^{mr}$$

whence $mr \mid n$ and $r \mid n$.

We now note that since $\mathbb{Z}/p\mathbb{Z}$ is a field by the results of the previous section we know that for any prime $p$ one has $\varphi(p) = p - 1$. In the case of $p^n$ for $n \geq 2$, We note that the only elements of $\mathbb{Z}/p^n\mathbb{Z}$ that are not invertible are those of the form $p^k$ for $k < n$. That is, elements in $\{p, p^2, \ldots, p^n\}$, where we associate $p^n$ with 0. Therefore,

$$\varphi(p^n) = p^n - p = p^{n-1}(p-1)$$

We now wish to establish multiplicativity[4] of $\varphi$. To prove this, it suffices to show that for co-prime integers $n, m$ one has the isomorphism of groups:

$$\mathbb{Z}_{nm}^* \cong \mathbb{Z}_n^* \times \mathbb{Z}_m^*$$

Certainly, we shall now define $\Gamma : \mathbb{Z}_{nm}^* \xrightarrow{\sim} \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ where

$$x \mapsto (x \bmod n, x \bmod m)$$

Clearly, this is a homomorphism of groups. We only need to show bijectivity. This is ultimately a consequence of the Chinese Remainder Theorem. To see

[3] If this is difficult to see use Euclid's lemma together with prime factorization!

[4] We wish to show that $\varphi(nm) = \varphi(n)\varphi(m)$ if $\gcd(n, m) = 1$.

that $\Gamma$ is injective we show that $\ker\Gamma \subseteq \{0\}$. Indeed, if $x \in \ker\Gamma$ then $x \equiv 0 \pmod{n,m}$ and so $n \mid x$ and $m \mid x$. By Euclid's lemma we glean $nm \mid x$ and hence $x \equiv 0 \pmod{nm}$. Now, to see that $\Gamma$ is surjective pick $(a,b) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. By the Chinese Remainder Theorem there is unique $x \in \mathbb{Z}/nm\mathbb{Z}$ such that $\Gamma(x) = (a,b)$. If $x$ shared a factor with, say, $nm$ by Euclid's lemma it would share a factor with one of $n, m$ contradicting that $\Gamma(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$.

Equipped with these notions we are able to prove the primitive root theorem.

### 1.4.2 Primitive root theorem

**Proposition 1.8** (Primitive Root Theorem)**.** *Let $p$ be a prime. Then $\mathbb{Z}_p^*$ is cyclic.*

Proof. We may verify the case directly for $p = 2$, as 1 generates the trivial group. Thus, assume that $p$ an odd prime. Then, we may write $p - 1 = \prod_{j=1}^{k} p_j^{e_j}$ for distinct primes $p_j$. Fix now some index $j$ relevant to this product. We wish to construct an element of $\mathbb{Z}_p^*$ with order $p_j^{e_j}$. To do this, we consider the following polynomials:

$$f_1(x) = x^{p_j^{e_j}} - 1 \pmod{p} \tag{6}$$

$$f_2(x) = x^{p_j^{e_j-1}} - 1 \pmod{p} \tag{7}$$

From our previous results we may find an $x_j \in \mathbb{Z}_p^*$ such that $f_1(x_j) \equiv 0 \pmod{p}$ but $f_2(x_j) \not\equiv 0 \pmod{p}$. This shows that $x_j$ has order $p_j^{e_j}$. Certainly, if this were not the case then $\ell := o(x_j) \mid p_j^{e_j}$, hence $\ell = p^\alpha$ for $\alpha < e_j$. Namely, for some small $\beta \geq 0$:

$$x^{p_j^{e_j-1}} \equiv x^{p_j^{\alpha+\beta}} \equiv x^{p_j^{\alpha} \cdot p_j^{\beta}} \equiv 1 \pmod{p}$$

which is a contradiction. Hence, $x_j$ has order $p_j^{e_j}$ in $\mathbb{Z}_p^*$. Noting that all the $p_j$ are co-prime we note that the product of all such $x_j$ must have order

$$\prod_{j=1}^{k} p_j e^{e_j} = p - 1 = \varphi(p)$$

and the result is proven.

◯

It may also be shown that $\varphi(\varphi(n))$ is the number of such group generators of $\mathbb{Z}_p^*$, although we shall omit this proof as it is quite uninteresting. This marks the end of our study of $\mathbb{Z}_p^*$.

## 2 Quadratic Congruences

We begin by defining a character on a group. Fix $n \in \mathbb{N}$. We may define a mapping:

$$\left(\frac{\cdot}{n}\right) : \mathbb{N} \to \{0, \pm 1\}, \quad x \mapsto \begin{cases} 1 & x \text{ is a square mod} n \\ -1 & x \text{ is not a square mod} n \\ 0 & \gcd(x,n) > 1 \end{cases} \tag{$\mathfrak{L}$}$$

Let now $p \in \mathbb{N}$ be a fixed prime, we consider the restriction of $\left(\frac{\cdot}{n}\right)$ to $\mathbb{Z}_n\mathbb{Z}^*$. This becomes a homomorphism of groups. Indeed, if $p = 2$ we are mapping from the trivial group $\mathbb{Z}_2^*$ and there is nothing to show. Suppose without harm that $p$ is an odd prime. It is now known that the group $\mathbb{Z}_p^*$ is cyclic and is generated by some element, $g$. That is, $\mathbb{Z}_p^* = \langle g \rangle$. We may therefore list the elements of $\mathbb{Z}_p^*$ *uniquely* as:

$$\mathbb{Z}_p^* = \left\{ g, g^2, \ldots, g^{\frac{p-1}{2}}, \ldots, g^{p-1} \right\}$$

It is now clear that all powers of $g$ with <u>even</u> exponent are squares, and all <u>odd</u> powers of $g$ are non-squares. Moreover, there are $\frac{p-1}{2}$ squares in this group.[5]. To verify that $\left(\frac{\cdot}{n}\right)$ is a homomorphism of groups it suffices to observe that $g^a g^b = g^{a+b}$ and $a + b$ is even if $a, b$ are both even or odd, and odd otherwise.

In practice we shall frequently make use of the following result:

**Theorem 2.1.** *Let $p$ be an odd prime and consider an integer $a$ such that $p \nmid a$. Then, $\left(\frac{a}{n}\right) = 1$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.*

Proof. Let us now denote the Legendre mapping shown in ($\mathfrak{L}$) by $\Gamma$. We define a second mapping:

$$\Phi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*, \quad a \mapsto a^{\frac{p-1}{2}} \tag{8}$$

We have shown above that $\Gamma$ is a homomorphism, we claim that $\Phi$ is as well. Of course, this follows immediately from the properties of exponentiation. Hence, from our general results from groups we know that $\ker \Phi < \mathbb{Z}_p^*$ and $\ker \Gamma < \mathbb{Z}_p^*$.[6] Now, by Lagrange's Theorem we know that $\# \ker \Phi \mid \varphi(p)$ and similarly for $\# \ker \Gamma$. We know from our above argument that

$$\# \ker \Gamma = \frac{\varphi(p)}{2}$$

We claim first of all that $\ker \Gamma \subseteq \ker \Phi$. Certainly, assume that $x \in \ker \Gamma$ so that $\left(\frac{x}{p}\right) = 1$ and hence that $x = y^2$ for some $y \in \mathbb{Z}_p^*$. Then, of course

$$\Phi(x) = x^{\frac{p-1}{2}} = y^{p-1} \equiv 1 \pmod{p}$$

implying that $x \in \ker \Phi$. Now, there is no integer dividing $p - 1$ larger than $\frac{p-1}{2}$, therefore to establish $\ker \Phi = \ker \Gamma$ it suffices to show $\ker \Gamma \subsetneq \mathbb{Z}_p^*$. To see that this is impossible, note that in that case one would find that

$$x^{\frac{p-1}{2}} - 1$$

has $p - 1$ roots: which cannot happen.

◯

[5] Half of them are square, and $p - 1$ is even.

[6] We write "$<$" to say "*subgroup of*".

Of course, we have the following relation in the case where $a = -1$:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{9}$$

Putting all of these together we glean the following:

**Criterion.** *For each odd prime $p$ and $x \in \mathbb{Z}_p^*$ is a square modulo $p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Similarly, $x$ has no square-root modulo $p$ if and only if $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$*

The proof is immediate from Fermat's little theorem, presented in the first section. The *Theorem of Quadratic Reciprocity* allows one to check whether a number is a square modulo a prime $p \geq 3$ quite easily and allows for some algebraic manipulations. We shall state but not prove this theorem:

**Theorem 2.2** (Quadratic Reciprocity)**.** *For distinct odd primes $p, q$ one has:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{$\mathfrak{Q}$}$$

# 3 Continued Fractions

In this section we devote ourselves to developing a basic understanding of continued fractions. For our purposes, we will be studying numbers of the form:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \tag{10}$$

where this expression may or may not terminate and $\{a_j\}_{j\geq 0} \subset (0, \infty)$. A suitable expression for the above is $[a_0, a_1, \ldots]$.

To make this notion precise and "neat" we require a more compact notion. Suppose that we define:

$$\begin{aligned} p_{-2} = 0, \quad p_{-1} = 1, \quad p_0 = a_0, \quad p_n = a_{n-1}p_{n-1} + p_{n-2} \\ q_{-2} = 1, \quad q_{-1} = 0, \quad q_0 = 1, \quad q_n = a_{n-1}p_{n-1} + p_{n-2} \end{aligned}$$

We now make the following claim regarding these continued fractions

**Proposition 3.1.** *Assume we have a continued fraction of the form $[a_0, a_1, \ldots, a_m]$ (where $m \leq \infty$). For each $n \leq m$ with $n < \infty$ one has:*

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n}$$

PROOF. We argue by induction on the lengths of these expressions $[a_0, \ldots, a_n]$. If $n = 0$ take any expression of the form $[a_0]$. It is clear that this agrees with $\frac{p_0}{q_0} = a_0$. Now assume the above holds for all expressions $[a_0, \ldots, a_{n-1}]$ for $n-1$. We wish to consider the case $n \in \mathbb{N}$. Let us write:

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = \left[a_0, \ldots, a_{n-1} + \frac{1}{a_n}\right]$$

On this last term we apply our induction hypothesis, to obtain:

$$\begin{aligned}
[a_0, a_1, \ldots, a_{n-1}, a_n] &= \frac{\left(a_{n-1} + \frac{1}{a_n}\right) p_{n-2} + p_{n-3}}{\left(a_{n-1} + \frac{1}{a_n}\right) q_{n-2} + q_{n-3}} \\
&= \frac{a_n(a_{n-1}p_{n-2} + p_{n-3}) + p_{n-2}}{a_n(a_{n-1}q_{n-2} + q_{n-3}) + q_{n-2}} \\
&= \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}
\end{aligned}$$

which concludes the proof.

◯

Although this gives us an expression for a partial continued fraction, it is not enough. We do not yet know in what ways these $p_j, q_j$ shall behave. For this, we give the following proposition:

**Proposition 3.2.** *Under the notation of the previous proposition, if $n \geq 0$ with $n \leq m$ we have*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \tag{11}$$
$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n \tag{12}$$

PROOF. We shall first prove (11) by induction on $n$. The case $n = 0$ is trivial and is a matter of verification. Assume (11) holds up to $n-1$. We now calculate the following expression

$$\begin{aligned}
p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\
&= q_{n-1} p_{n-2} - p_{n-1} q_{n-2} \\
&= -(p_{n-1} q_{n-2} - q_{n-1} p_{n-2}) \\
&= -(-1)^{n-2}
\end{aligned}$$

To show equation (12) we may employ a direct calculation

$$\begin{aligned}
p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\
&= a_n(p_{n-1} q_{n-2} - q_{n-1} p_{n-1})
\end{aligned}$$

which by our first equation is equal to $a_n(-1)^{n-2} = a_n(-1)^n$.

◯

We note that these two equations give us other relations. Primarily, we deduce from (11)-(12) the following equations:

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \tag{13}$$

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = a_n \frac{(-1)^n}{q_n q_{n-2}} \tag{14}$$

Now, we observe that all representations of the form $\frac{p_n}{q_n}$ where $n \in \mathbb{N}$ corresponds to a fraction in reduced terms. That is, $\gcd(p_n, q_n) = 1$ for all $n \in \mathbb{N}$. To see this, assume $d \mid p_n$ and $d \mid q_n$. Thence, by (11) it follows that $d \mid (-1)^{n-1}$ and that $d = \pm 1$.

### 3.1 Sequence of Partial Convergents

Throughout the remainder of this section let us consider some continued fraction $[a_0, \ldots, a_m]$ with $m = \infty$ being admissible. For finite $n \leq m$ we write

$$c_n := \frac{p_n}{q_m} = [a_0, \ldots, a_n]$$

to denote the $n^{th}$ *partial convergent*. This part of the text is devoted to studying their *convergence*. We require that the reader have some knowledge of basic real analysis.

**Proposition 3.3.** *The even-indexed subsequence $(c_{2n})$ increases strictly with $n$ and the odd-indexed subsequence $(c_{2n+1})$ decreases strictly with $n$. Meanwhile, all odd indexed elements are no-smaller than any even indexed $c_n$.*

Proof. Strict monotonicity is easy. We write by (14)

$$c_n - c_{n-2} = a_n \frac{(-1)^n}{q_n q_{n-2}}$$

If $n$ is even, the RHS is $> 0$ and if $n$ is odd the RHS is always $< 0$. Hence, we have proven the first claim. For the second, assume we have integers $r, s$ such that $c_{2r+1} < c_{2s}$. We note that $r \neq s$ for in this case one would have

$$c_{2s+1} - c_{2s} < 0$$

directly contradicting (13). Furthermore, $r > s$ is impossible for then we may write

$$c_{2r+1} < c_{2s} < c_{2r}$$

again in contradiction with (13). Finally, to see that $r < s$ is impossible write by our equation in (13)

$$c_{2r} < c_{2s} < c_{2s+1} < c_{2r+1}$$

which is a contradiction.

$\bigcirc$

Note that the point of this is not moot. There are *many* numbers with an infinite fraction representation. Trivially, each $x \in \mathbb{Z} \setminus \{0\}$ has a representation. Perhaps a better claim is that each element of $\mathbb{Q}$ has a representation of the form in (10). It is even possible to derive an algorithm for computing such a representation. Consider some rational $x = \frac{a}{b}$ and suppose without harm that $\gcd(a, b) = 1$.

By Euclid's algorithm we write $a = a_0 b + r_0$ with $0 \leq r_0 < b$. Now, this implies that $\frac{a}{b} = a_0 + \frac{r_0}{b}$. Now, we set $t_0 := \frac{1}{b/r_0}$. Then,

$$x = a_0 + \frac{1}{b/r_0}$$

Repeat this procedure with $b/r_0$ indefinitely and we glean our representation. It turns out that a similar procedure applies that to any non-zero real number $x$. Let now $x > 0$ and write

$$x = a_0 + t_0, \quad a_0 = \lfloor x \rfloor, \, t_0 := x - a_0$$

Then, $0 \leq t_0 < 1$. If $t_0 = 0$ then we are done, else take $1/t_0$ so that $x = a_0 + \frac{1}{1/t_0}$ and repeat this process indefinitely on $1/t_0$. What we wish to study is how the partial convergents behave as $n \to \infty$. Observe that in the indefinite continuation of our algorithm/procedure above for computing the continued fractional representation of a positive real number $x$ we have trivially

$$[a_0, a_1, \ldots, a_n + t_n] = \left[a_0, a_1, \ldots, a_n, \frac{1}{t_n}\right]$$

We now give our result:

**Theorem 3.4.** *Let $\{a_j\}_{j \geq 0} \subseteq \mathbb{N}$ be a sequence of coefficients for a continued fraction representation. Then,*

$$\lim_{n \to \infty} c_n < \infty$$

*exists.*

Proof. Here we show that both subsequences $(c_{2n}), (c_{2n+1})$ converge to the same limit. Note that by a previous result both of these are monotonic sequences. Moreover, they are bounded trivially; i.e. $c_{2n} \leq c_1$ and $c_{2n+1} \geq c_2$. This ensures that the limits:

$$\alpha := \lim_{n \to \infty} c_{2n} \quad \text{and} \quad \beta := \lim_{n \to \infty} c_{2n+1}$$

exist and are finite. We wish to show that they are the same, i.e. $\alpha = \beta$. To see this, let $n$ be large enough ($n \geq 3$ should suffice):

$$|c_{2n+1} - c_{2n}| \overset{(13)}{=} \frac{1}{|q_{2n+1} q_{2n}|} \leq \frac{1}{(2n+1)(2n)} \xrightarrow{n \to \infty} 0 \qquad (\dagger)$$

$\bigcirc$

From this theorem we observe that it "makes sense" to define $[a_0, a_1, \ldots] := \lim c_n$.

A sufficient condition for the convergence of the continued fraction goes as follows:

**Proposition 3.5.** *Let $\{a_j\}_{j\geq 0} \subset (0,\infty)$ such that $\sum_{j\geq 0} a_j = \infty$. Then, $\lim c_n$ exists and is finite.*[7]

Proof. We note from the previous proof that it suffices to show that $\frac{1}{q_{2n+1}q_{2n}} \to 0$ as $n \to \infty$, we merely required that the integers be integral valued to have the useful estimate in (†). Now, we assume that

$$\sum_{j\geq 0} a_j = \infty$$

Assume $n$ is large and even. Then,

$$q_n = a_n q_{n-1} + q_{n-2} = a_n q_{n-1} + a_{n-2}q_{n-3} + q_{n-4} + \cdots$$

That is, $q_n = a_n q_{n-1} + a_{n-2}q_{n-3} + a_{n-4}q_{n-5} + \cdots$ and we obtain even indexed $a_j$ up to $n$. Now, since $q_0 \geq 1$ and the $q_j$ are monotone increasing we obtain that $q_n \geq a_n + a_{n-2} + \cdots + a_2$. Similarly, if $n$ is odd we obtain:

$$q_n \geq a_{n-2} + a_{n-3} + \cdots + a_1$$

As the series $\sum_{j\geq 0} a_0 = \infty$ at least one of $\sum_{j \text{ odd}} a_j$ or $\sum_{j \text{ even}} a_j$ "diverges" to infinity. Therefore, one of $q_{2n}$ or $q_{2n+1}$ tends to infinity as $n \to \infty$.

◯

We are finally at the point where we may show that the infinite fraction procedure given for a general real number $x$ makes sense.

**Lemma 3.6.** *Let $x$ be a real number and $\{c_n\}$ the sequence of partial convergents generated by the algorithm given. Then for any $n \in \mathbb{N}$,*

$$|x - c_n| < \frac{1}{q_n \cdot q_{n+1}}.$$

Proof. We handle the case where the representation is infinite, for otherwise in each step we have equality and hence must preserve this equality in the last step. In this case, it is obvious that $x \in \mathbb{Q}$.

In the procedure at the $n^{\text{th}}$ step we found that

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n + t_n}}}}$$

[7]This proposition has a converse, but we omit this.

and hence, $x = [a_0, a_1, \ldots, a_{n-1}, a_n + t_n] = \left[a_0, a_1, \ldots, a_n, \frac{1}{t_n}\right]$. These are precisely the $\{c_n\}$ generated by the process. Now, we may write out

$$x = \frac{\frac{1}{t_n} \cdot p_n + p_{n-1}}{\frac{1}{t_n} \cdot q_n + q_{n-1}}$$

Now, let us estimate the difference for all $n \gg 0$:

$$|x - c_n| = \left|\frac{p_n + t_n p_{n-1}}{q_n + t_n q_{n-1}} - \frac{p_n}{q_n}\right| = \left|\frac{t_n p_{n-1} q_n - t_n q_{n-1} p_n}{q_n(q_n + t_n q_{n-1})}\right| \overset{(13)}{=} \frac{t_n}{q_n(q_n + t_n q_{n-1})}$$

However, this last term is precisely:

$$\frac{1}{q_n\left(\frac{1}{t_n} q_n + q_{n-1}\right)} < \frac{1}{q_n(a_{n+1} q_n + q_{n-1})} = \frac{1}{q_n \cdot q_{n+1}}$$

◯

**Theorem 3.7.** *Let $x > 0$ be a real number and $\{c_n\}$ the sequence of partial convergents generated by the algorithm given. Then, $c_n \to x$ as $n \to \infty$.*

Proof. From the previous, lemma, we have

$$|x - c_n| < \frac{1}{q_n \cdot q_{n+1}}.$$

Note that the right hand side of this equation tends to zero as $n$ tends to infinity implying the result.

◯

### 3.2 Sums of Two Squares

This section is devoted to proving the following theorem:

**Theorem 3.8.** *An integer $n$ is the sum of two squares if and only if every prime $p \equiv 3 \bmod 4$ has an even exponent in its prime factorization of $n$.*

Given an integer $x > 0$ we shall say a representation is *primitive* provided it is of the form $n = x^2 + y^2$ for integers $x, y$ co-prime. Our first claim is the following:

**Lemma 3.9.** *If $n \geq 2$ has a prime factor $p$ with $p \equiv 3 \bmod 4$ then $n$ has no primitive representations.*

Proof. By way of contradiction, assume we may write $n = x^2 + y^2$ with $x, y \neq 0$ co-prime. Note then that $p \nmid x$ and $p \nmid y$ for if $p$ divided, say, $x$ we would obtain that $p \mid (n - x^2) = y^2$ and hence $p \mid y$, implying that $\gcd(x, y) > 1$. It follows that $y^2$ (or $x^2$) is a unit modulo $p$, i.e an element of the multiplicative group $\mathbb{Z}_p^*$ and therefore admits an inverse $y^{-2}$. Therefore, since $p \mid n$ we find

$$n \equiv 0 \equiv x^2 + y^2 \pmod{p} \implies \left(\frac{x}{y}\right)^2 + 1 \equiv 0 \pmod{p}$$

In particular, $\left(\frac{-1}{p}\right) = 1$. On the other-hand, we may write $p - 1 = 2 + 4k$ where $k \in \mathbb{Z}$. Then, by Euler's Criterion we notice that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1 \neq 1$$

a contradiction.

◯

We now wish to prove the subsequent implication:

**Proposition 3.10.** *Let $n$ be the sum of two squares. Then all primes $p \mid n$ reducing to* 3 mod 4 *have even exponent in the prime factorization of $n$.*

Proof. We argue by contradiction. Suppose that there is some $p \equiv 3 \bmod 4$ with $p^r \parallel n$ with $r$ odd. Now, since $n$ is the sum of two squares we may write for $x, y \neq 0$ integers:

$$n = x^2 + y^2$$

Set $d := \gcd(x, y)$. Then there are integers $x', y'$ respectively such that $x = dx_0$ and $y = dy_0$. Therefore, for some $n_0 \in \mathbb{N}$ we have:

$$n = x^2 + y^2 = d^2(x_0^2 + y_0^2) = d^2 n_0$$

and $\gcd(x_0, y_0) = 1$. However, as $r$ was odd $p \mid n_0$. This is a primitive expression, which contradicts the previous lemma.

◯

**Lemma 3.11.** *For every $x \in \mathbb{R}$, $n \in \mathbb{N}$, there exists integers $a, b$ with $1 \leq b \leq n$ such that*

$$\left|x - \frac{a}{b}\right| \leq \frac{1}{b \cdot (n+1)}$$

Proof. From lemma 3.6, we have for any $m \in \mathbb{N}$,

$$|x - c_m| < \frac{1}{q_m \cdot q_{m+1}}.$$

As the sequence of denominators $q_m$ is strictly increasing and $q_0 = 1$, we can find $m \in \mathbb{N}$ such that $q_m \leq n < q_{m+1}$. Letting $a = p_m$ and $b = q_m$ we obtain

$$\left|x - \frac{a}{b}\right| = |x - c_m| < \frac{1}{b \cdot q_{m+1}} \leq \frac{1}{b \cdot (n+1)}$$

as desired.

◯

**Lemma 3.12.** *Any prime $p$ reducing to* 1 *modulo* 4 *is the sum of two square.*

PROOF. First note that for any such prime, we have

$$\left(\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$

Therefore, there exists an integer $r \in \{1, \ldots, p-1\}$ such that $r^2 \equiv 1 \bmod p$. We now use the previous lemma with $x = -r/p$ and $n = \lfloor \sqrt{p} \rfloor$. Let $a, b$ be integers such that $1 \leq b \leq n$ and

$$\left| -\frac{r}{p} - \frac{a}{b} \right| \leq \frac{1}{b \cdot (n+1)} < \frac{1}{b\sqrt{p}}.$$

Define $c = rb + pa$, then we will show that $p = b^2 + c^2$ thereby proving the lemma. We first note that

$$b^2 + c^2 \equiv b^2(r^2 + 1) \equiv b^2(-1 + 1) \equiv 0 \mod p. \tag{1}$$

Moreover, we have

$$|c| = |bp| \cdot \left| -\frac{r}{p} - \frac{a}{b} \right| < \frac{bp}{b\sqrt{p}} = \frac{1}{\sqrt{p}}.$$

It follows that

$$1 \leq b^2 + c^2 < 2\,(\sqrt{p})^2 = 2p \tag{2}$$

Putting equations (1) and (2) together, we obtain $b^2 + c^2 = p$.

◯

**Proposition 3.13.** *Let $n$ be such that all primes $p \mid n$ reducing to $3 \bmod 4$ have even exponent in the prime factorization of $n$, then $n$ is the sum of two squares.*

PROOF. We begin by noting that if $n = ab$ where $a$, $b$ are integers which can be written as the sum of two squares, then

$$n = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$$

Now let $n_0$ be the maximal integer such that $n = n_0^2 m$ for some integer $m$. Then it is sufficient to show that $m$ is the sum of two squares. By assumption, if $p$ is a prime divisor of $m$ then $p$ reduces to 1 modulo 4. By the previous lemma, we therefore know that $p$ can be written as the sum of two squares. By our initial remark, this implies that $m$ can be written as a sum of squares.

◯

Finally, our original theorem follows from Propositions 3.10 and 3.13

### 3.3 Pell's equation

In this section, we study in $\mathbb{N}$ Pell's equation, which is of the form

$$x^2 - ny^2 = 1.$$

For fixed $n$, we ask what are all the solution $x, y$ such that the above equation holds. We will only consider positive solutions since $x$ and $y$ are squared!

We first remark that if $n = d^2$ for some integer $d$, then

$$x^2 - ny^2 = (x - dy)(x + dy) = 1 \quad \text{if and only if } x = 1,\ dy = 0.$$

Suppose now that $n$ is not a perfect square, then how can one find the continued fraction of $\sqrt{n}$? Begin by denoting $d = \lfloor \sqrt{n} \rfloor$, then one can show that the continued fraction of $\sqrt{n}$ can be expressed by $[d, \overline{a_1, \ldots, a_{k-1}, a_k, a_{k-1}, \ldots, a_1, 2d}]$ for some integers $a_1, a_2, \ldots a_k$. Let $\ell = 2k$ be the minimal period for such a continued fraction, then

$$(x_1, y_1) = \begin{cases} (p_{\ell-1}, q_{\ell-1}) & \text{if } k \text{ is even} \\ (p_{2\ell-1}, q_{2\ell-1}) & \text{if } k \text{ is odd} \end{cases}$$

is a minimal solution, i.e. a solution such that $x$ is minimal. All other solutions are given by

$$x + \sqrt{n}y = \left(x_1 + \sqrt{n}y_1\right)^m$$

Seeing that the above indeed provides solutions to Pell's equation can be shown by induction. The converse is left to be read in other books, where the author had more patience.[‡]

## 4 Diophantine approximations

We state theorems without proof. We begin by reminder the reader of the definition of an algebraic number: $x \in \mathbb{R}$ is algebraic if it is the root of a polynomial with integer coefficients.

**Definition 1** (Liouville)**.** *A Liouville number is an irrational number $x$ if there exists a constant $c > 0$ such that for all $n \in \mathbb{N}$ we may find a rational number $\frac{p}{q}$ such that:*

$$\left| x - \frac{p}{q} \right| \leq \frac{c}{q^n}$$

*where $q > 1$.*

We claim the following, in the hopes of obtaining a method for proving that certain numbers are transcendental. Note first of all that requiring $x$ to be irrational in the above definition is of no great harm, since we will show below that all Liouville numbers are transcendental, and all transcendental numbers are irrational, in any case.

**Theorem 4.1.** *Any Liouville number is transcendental.*

PROOF. Here we argue by contradiction. Let $\eta$ be a Liouville number. We construct a sequence of integers $(p,q)_n$ as follows: for $n \in \mathbb{N}$ pick a pair $(p,q) \in \mathbb{Z}^2$ with $q > 1$ such that

$$\left|\eta - \frac{p}{q}\right| \leq \frac{c}{q^n}$$

Assume now that there is some $f \in \mathbb{Z}[x]$ with $m = \deg f$ and $f(\eta) = 0$. Note that $f$ has at-most $m$ roots in $\mathbb{R}$, and hence at most finitely many of these $(p,q)$ correspond to rational roots of this polynomial $f$, for otherwise in passing to a constant subsequence $\{(p,q)\}$ one would have $\eta = \frac{p}{q} \in \mathbb{Q}$. Hence, we only need handle the case for all large $n$.

Now, since $f$ is a polynomial it is $C^\infty(\mathbb{R})$ and therefore Lipschitz continuous with constant $L > 0$ on any large compact interval about $\eta$. Observe that since $f \in \mathbb{Z}[x]$ we trivially have for all $(p,q)$ associated to $n$ large:

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^m}$$

Therefore,

$$\frac{1}{q^m} \leq \left|f\left(\frac{p}{q}\right)\right| = \left|f(\eta) - f\left(\frac{p}{q}\right)\right| \leq L\left|\eta - \frac{p}{q}\right| \leq \frac{Lc}{q^n}$$

and taking $n$ large gives a contradiction.

$\bigcirc$