Introduction to Number Theory

5CCM224A, Fall 2019[1]

Salman Ahmad Faris

King's College London

E-mail: salman.faris@kcl.ac.uk

[1] *based on lectures by James Newton. These notes, however, have been altered strongly after the lectures. In particular, some proofs were filled in by me; and some of the contents were adjusted so that organization is prioritized and things are coherent. All errors are surely mine, feel free to email me if you spot any.*

Contents

Notation. The two most important notation is $\mathbb{N}$ and $\mathbb{Z}$ which are the set

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}, \quad \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}.$$

Note that we do **not** include 0 in $\mathbb{N}$. This is a choice. Some books may put 0 in $\mathbb{N}$. Whenever we say that $n \in \mathbb{N}$, we may write $n > 0$. Whenever we say that $n \in \mathbb{N} \cup \{0\}$, we may write $n \geqslant 0$.

References. Together with the lectures, the following books were useful references in the making of this notes:

(1). J. H. Silverman, *A Friendly Introduction to Number Theory*, Pearson.

(2). K. H. Rosen, *Elementary Number Theory and Its Applications*, Pearson.

(3). G. A. Jones, J. M. Jones, *Elementary Number Theory*, Springer.

PART

I

Setting the table

1 Divisibility

Definition 1.1. Let $a, b \in \mathbb{Z}$. We say that b **divides** a if there exists an integer $q \in \mathbb{Z}$ such that $a = qb$. If b divides a, we write $b \mid a$.

Let's talk about some basic properties.

Fact. Let $a, b, c \in \mathbb{Z}$.

1. (Transitivity) If $a|b$ and $b|c$, then $a|c$.
2. If $a|b$ and $a|c$, then $a|(bx + cy)$ for all $x, y, \in \mathbb{Z}$.
3. If $a|1$, then $a = \pm 1$
4. If $a|b$ and $b|a$, then $a = \pm b$.
5. Suppose $c \neq 0$. Then $a|b \iff ac|bc$.

Exercise. Prove these properties. You only require the definition above.

Fact. (Well-ordering Principle). Every non-empty subset $S \subseteq \mathbb{N}$ has a least element.

Remark. The well-ordering Principle also holds for $\mathbb{N} \cup \{0\}$. It does **not** work for $\mathbb{Z}$.

Theorem 1.1. (Division Algorithm). Let $a, b \in \mathbb{Z}$ with $b > 0$. Then, there exists unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leqslant r < b$.

Proof. **Existence.** Let $S = \{a - nb : n \in \mathbb{Z}\}$. Since S contains positive elements, it has a least element, r by the well-ordering principle. So, $r = a - qb$ for some $q \in \mathbb{Z}$. Now, $0 \leqslant r < b$, otherwise $r - b$ is a smaller non-negative element of S. **Uniqueness.** If $a = qb + r = q'b + r'$, then $b|(r - r')$ and $-b < r - r' < b$ so this implies that $r = r'$ and thus $q = q'$. This proves uniqueness of q and r. ∎

S looks like: $\ldots, a - 3b, a - 2b, a - b, a + b, a + 2b, a + 3b, \ldots$

1.1 Greatest Common Divisors

Definition 1.2. Let $a, b \in \mathbb{Z}$ not both zero. Then, the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$ is defined to be the largest integer d such that $d|a$ and $d|b$.

Remark. We do not define $\gcd(0, 0)$. This is because any number is a divisor of 0, so there is no such *greatest* common divisor.

Exercise. Prove that

1. $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b) = \gcd(|a|, |b|)$.

2. $\gcd(a, 0) = |a|$.

3. If $b|a$, then $\gcd(a, b) = |b|$. This is quite obvious.

Lemma 1.2. Let $a, b \in \mathbb{Z}$ not both zero. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$ for any $q \in \mathbb{Z}$.

Theorem 1.3. (Bezout's lemma). Let $a, b \in \mathbb{Z}$ not both zero. Then, there exist integers u, v such that

$$\gcd(a, b) = au + bv$$

Proposition 1.1. Let $a, b \in \mathbb{Z}$ not both zero and consider the set

$$S = \{au + bv : u, v \in \mathbb{Z}\}$$

Let $d > 0$ be the smallest positive integer in S. Then, $d = \gcd(a, b)$.

Remark. Two consequences of this Proposition:

1. $\exists\, u, v \in \mathbb{Z}$ such that $\gcd(a, b) = au + bv$ (We recovered Bezout's lemma).
2. $\gcd(a, b) = 1$ if and only if $\exists\, u, v \in \mathbb{Z}$ such that $1 = au + bv$.

Corollary 1.1. Let $a, b \in \mathbb{Z}$ not both zero. Let $d \in \mathbb{Z}$. Then, d is a common divisor of a and b if and only if $d|\gcd(a, b)$.

1.2 Coprimality

Definition 1.3. Let $a, b \in \mathbb{Z}$. We say that a and b are **coprime** (or relatively prime) if $\gcd(a, b) = 1$.

Lemma 1.4. Suppose a, b are coprime integers. Then

1. If $a|c$ and $b|c$, then $(ab)|c$.
2. If $a|bc$, then $a|c$ where $c \in \mathbb{Z}$.
3. Suppose $c \in \mathbb{Z}$ such that a and c are coprime, then a and bc are coprime.

1.3 Least Common Multiples

Definition 1.4. If $a, b \in \mathbb{Z}$, then a **common multiple** of a and b is an integer $c \in \mathbb{Z}$ such that $a|c$ and $b|c$.

Definition 1.5. If $a, b \in \mathbb{Z}$ both non-zero, then the **least common multiple** of a and b is, denoted $\text{lcm}(a, b)$, is the smallest positive integer which is a common multiple of a and b

Remark. $\text{lcm}(a, b)|m \iff a|m$ and $b|m$.

Remark. Despite being defined to be the **smallest** positive integer such that it is a common multiple of two integers, it is **not necessarily small**. $\text{lcm}(7, 13) = 91$.

Proposition 1.2. Let $a, b \in \mathbb{Z}$ both non-zero. Then,

$$\gcd(a, b) \cdot \text{lcm}(a, b) = |ab|$$

1.4 Linear Diophantine Equations

Theorem 1.5. Let $a, b, c \in \mathbb{Z}$ with a, b not both zero and let $d = \gcd(a, b)$. The equation

$$ax + by = c$$

has an integer solution (x, y) if and only if $d|c$. In fact, if (x_1, y_1) is one solution, then all the solutions are given by

$$\left(x_1 + \frac{kb}{d}, y_1 - \frac{ka}{d}\right) \quad \text{for } k \in \mathbb{Z}$$

Moreover, if $d|c$, then the equation has infinitely many solutions.

Proposition 1.3. Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Consider the linear congruence $ax \equiv b \pmod{m}$.

(1). The congruence is solvable if and only if $\gcd(a, m) \mid b$.

(2). If the congruence is solvable, then it has $\gcd(a, m)$ residues classes modulo m as solutions.

(3). If λ is a solution, then $x \equiv \lambda \pmod{\frac{m}{\gcd(a,m)}}$ are all the solutions.

Proof. Exercise. ∎

2 Prime Numbers

Definition 2.1. An integer $p > 1$ is called a **prime number** or just a **prime** if it has no positive divisors other than 1 and p itself. An integer $n > 1$ is called a **composite** if it is not prime.

Remark. 1 is neither a prime nor a composite. This is a convention.

Lemma 2.1. (Euclid's Lemma). Let p be a prime number and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Then,

$$p|(a_1 a_2 \cdots a_n) \implies p|a_i \text{ for some } i$$

Theorem 2.2. (Fundamental Theorem of Arithmetic). Every integer $n > 1$ can be expressed uniquely (up to reordering) as a product of primes.

Lemma 2.3. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where p_i distinct primes and $a_i \geqslant 0$. Then,

1. $d > 0$ is a divisor of n if and only if

$$d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

   with $0 \leqslant b_i \leqslant a_i$ for each i.

2. The number of positive divisors of n is $\prod_{i=1}^{r}(a_i + 1)$.

Lemma 2.4. Let $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ where $a_i, b_i \geqslant 0$. Then,

1. $\gcd(m, n) = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_r^{\varepsilon_r}$ where $\varepsilon_i = \min(a_i, b_i)$.
2. $\operatorname{lcm}(m, n) = p_1^{\eta_1} p_2^{\eta_2} \cdots p_r^{\eta_r}$ where $\eta_i = \max(a_i, b_i)$.

Theorem 2.5. (Euclid). There are infinitely many primes.

Proposition 2.1. There are arbitrarily large gaps between consecutive primes. More precisely, if $k \geqslant 2$ is an integer, then there are k consecutive integers which are composite.

Lemma 2.6. Let $n = \prod_{i=1}^{r} p_i^{a_i}$ be the prime factorization of n. Then d is a positive divisor of n if and only if d has the form

$$d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

where $0 \leqslant b_i \leqslant a_i$ for all $1 \leqslant i \leqslant k$.

Proof. Suppose $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_k^{\lambda_k}$ where b_i, λ_j are non-negative integers and $p_1, \ldots, p_r, q_1, \ldots, q_k$ are distinct primes. Now

$$d \mid n \iff \frac{n}{d} \in \mathbb{Z} \iff \frac{n}{d} = p_1^{a_1 - b_1} p_2^{a_2 - b_2} \cdots p_r^{a_r - b_r} q_1^{-\lambda_1} q_2^{-\lambda_2} \cdots q_k^{-\lambda_k} \in \mathbb{Z}.$$

Now this is true if and only if $a_i - b_i \geqslant 0$ for all $1 \leqslant i \leqslant r$ and that $\lambda_j = 0$ for all $1 \leqslant j \leqslant k$, as desired. ∎

Lemma 2.7. Let $a, b \in \mathbb{N}$. Then we may write a and b as products of powers of the same list of primes, but with the powers allowed to be 0.

Proof. Let p be the biggest prime divisor of a and b. Suppose p is the r-th prime number and let $p = p_r$. Now consider all the prime numbers up to and including p i.e. the list $p_1, p_2, \ldots, p_r$. Then by the Fundamental Theorem of Arithmetic, we can write

$$a = p_1^{a_1} \cdots p_r^{a_r} \qquad \text{and} \qquad b = p_1^{b_1} \cdots p_r^{b_r},$$

for some non-negative integers a_i, b_i, because every prime divisor of a and b is in the list $p_1, \ldots, p_r$ (as we assumed $p = p_r$ is the biggest prime divisor). If say p_i doesn't appear in the prime factorisation of either a or b or both, then we let the power of p_i to be 0. ∎

Theorem 2.8. Let $a, b \in \mathbb{N}$ and $n \in \mathbb{N}$. Then $a^n \mid b^n$ if and only if $a \mid b$.

Proof. The reverse direction is trivial. If $a|b$, then $b = ak$ for some $k \in \mathbb{Z}$. So, $b^n = a^n k^n$ and hence $a^n \mid b^n$. Conversely, by the preceding lemma, we may write

$$a = \prod_{i=1}^{r} p_i^{a_i} \qquad \text{and} \qquad b = \prod_{i=1}^{r} p_i^{b_i},$$

where p_i are all distinct primes, and $a_i, b_i \geqslant 0$ for all i. Then

$$a^n = \prod_{i=1}^{r} p_i^{n a_i} \qquad \text{and} \qquad b^n = \prod_{i=1}^{r} p_i^{n b_i}.$$

By hypothesis $a^n | b^n$ and so $b^n / a^n \in \mathbb{Z}$. Now observe that

$$\frac{b_n}{a_n} \in \mathbb{Z} \iff p_1^{n(b_1 - a_1)} \cdots p_r^{n(b_r - a_r)} \in \mathbb{Z}.$$

This is true if and only if $n(b_i - a_i) \geqslant 0$ for all i which implies $b_i \geqslant a_i$ for all i. But this condition gives $b/a \in \mathbb{Z}$ so $a|b$, as desired. ∎

the implication is because $n > 0$

PART

II

Developing our arsenal

3 Congruences

Definition 3.1. Let m be a non-zero integer and let $a, b \in \mathbb{Z}$. We say a is **congruent** to b modulo m if $m|(a-b)$. We write this as $a \equiv b \pmod{m}$.

Remark. We first see some basic properties of being *congruent*.

1. Congruence is an equivalence relation.
2. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. Moreover, $ax + cy \equiv bx + dy \pmod{m}$ for all $x, y \in \mathbb{Z}$.
3. If $d|m$, then $a \equiv b \pmod{m} \implies a \equiv b \pmod{d}$.
4. If $a \equiv b \pmod{m}$ and $c \neq 0 \implies ac \equiv bc \pmod{mc}$.

Definition 3.2. Let $m \in \mathbb{N}$. The set $\{x_1, x_2, \ldots, x_r\}$ is called a **complete residue system modulo** m if for all $y \in \mathbb{Z}$ there exists exactly one x_i such that $y \equiv x_i \pmod{m}$.

Remark. (Very "surprising" Fact). In general, every complete residue system modulo m has size m.

Definition 3.3. Let m be a non-zero integer and $a \in \mathbb{Z}$. The **residue class of** a or **congruence class of** a is the set:

$$[a]_m = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\}$$

Lemma 3.1.

$$[a]_m = [b]_m \iff a \equiv b \pmod{m}$$

Proof. Straight from definitions. ∎

Definition 3.4. Let $m \in \mathbb{N}$. Denote $\mathbb{Z}_m$ to be the set of congruence classes modulo m.

Remark. ($\mathbb{Z}_m$ Representations). We can write $\mathbb{Z}_m$ the following way:

1. $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$
2. If $\{x_1, x_2, \ldots, x_m\}$ is *any* complete residue system modulo m, then
$$\mathbb{Z}_m = \{[x_1]_m, [x_2]_m, \ldots, [x_m]_m\}$$

Definition 3.5. Let m be a non-zero integer and $a, b \in \mathbb{Z}$. We define the addition and multiplication operations on $\mathbb{Z}_m$ by:

1. $[a]_m + [b]_m = [a+b]_m$
2. $[a]_m \cdot [b]_m = [a \cdot b]_m$

These (binary) operations are indeed well-defined. It is an exercise to check that this is indeed true.

4 Solving equations in $\mathbb{Z}_m$

A problem that motivates us is the following.

"*Let $f \in \mathbb{Z}[X]$. Can we show that the equation $f(X) = 0$ has an integer solution?*"

One way of seeing this equation **does not** have a solution is by showing that if there exists a particular m such that the equation has no solutions modulo m, then the equation must have no integer solutions at all. This leads us to the next problem.

"*Given a polynomial $f \in \mathbb{Z}[X]$ and an integer m. Can we find all integers $a \in \mathbb{Z}$ such that m divides $f(a)$? That is, can we find $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \pmod{m}$?*"

Well, it was easy when $f(X) = 0$ is a linear Diophantine equation, but how about to solve a more complicated one like $X^2 + 3X + 5 = 0$?

Lemma 4.1. Let $f \in \mathbb{Z}[X]$. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Proof. Suppose $f(x) = c_0 + c_1X + \ldots + c_nX^n$. Now, $a \equiv b \pmod{m} \implies a^i \equiv b^i \pmod{m}$ for any $i \geqslant 0$. Moreover, $c_ia^i \equiv c_ib^i \pmod{m}$. Adding these togethers, we have that $f(a) \equiv f(b) \pmod{m}$. ■

Although it is not very obvious at first sight, this lemma actually gives an answer to our previous question. It gives us the important fact that to find all integers a such that $f(a) \equiv 0 \pmod{m}$, we just need to find **one single** a that satisfies $f(a) \equiv 0 \pmod{m}$ **for each congruence class**. Once we find (or not) such an a for each congruence class, all the other members of that congruence class also solves (or does not) $f(X) \equiv 0 \pmod{m}$.

Remark. (Handy tool). A handy tip for solving equations $f(X) \equiv 0 \pmod{m}$ in $\mathbb{Z}_m$ is **reduction modulo m**. This is done by viewing the polynomial with coefficients reduced modulo m. This is handy with the realization that we are actually finding roots for $f(X)$ with coefficients in $\mathbb{Z}_m$.

To see this, $f(a) \equiv 0 \pmod{m} \iff c_0 + \ldots + c_na^n \equiv 0 \pmod{m} \iff [c_0 + \ldots + c_na^n]_m = [0]_m \iff [c_0]_m + [c_1]_m[a]_m + \ldots + [c_n]_m[a]_m^n = [0]_m$.

Example. Let $f(X) = X^2+1$ and consider the solutions to $f(X) \equiv 0 \pmod{3}$. There are really only 3 set of congruence classes mod 3 so we can try each representative (of the classes) – obviously 0, 1 and 2 – to see that there are no solutions to $f(X) \equiv 0 \pmod{3}$.

Example. Let $f(X) = X^2 + 1$ but now consider the solutions to $f(X) \equiv 0 \pmod{5}$. Brute forcing, we can see that 2 and -2 solves this equation. By the lemma above, $7, 12, 17, 22, 27, \ldots$ and $3, 8, 13, 18, 23, 28, \ldots$ all solves the equation as well i.e. integers congruent to 2 and -2 modulo 5.

Example. Let's try a harder example. Let $f(X) = X^5 - X^2 + X - 3$ and consider the solutions to $f(X) \equiv 0 \pmod{4}$. Again, there are only 4 elements in $\mathbb{Z}_4$ so we can brute force. But instead of brute forcing $0, 1, 2, 3$, recalling the remark ($\mathbb{Z}_m$ Representations), since $\{-1, 0, 1, 2\}$ is a complete residue system (modulo 4), we can brute force these values instead.

$$\begin{aligned} f(-1) = -6 \equiv 2 \pmod 4 \\ f(0) = -3 \equiv 1 \pmod 4 \\ f(1) = -2 \equiv 2 \pmod 4 \\ f(2) = 27 \equiv 2 \pmod 4 \end{aligned}$$

Hence, we conclude that there no solutions to $f(X) \equiv 0 \pmod 4$. Consequently, there are no solutions to $f(X) = 0$.

4.1 Chinese Remainder Theorem

Notice the fact that we have been **brute-forcing** in all the examples above. A natural question is, how do we do it if the modulus m is extremely large? Brute-forcing would not fail, but will take an immense amount of time so we need a more efficient method. Thankfully, this is tackled using a machinery called the Chinese Remainder Theorem. This tool dates back to a third century problem posed by the Chinese mathematician Sun tzu:

"*There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?*"

An equivalent way of stating the problem posed by Sun tzu using modern number theory is, what are the numbers x such that:

$$\begin{aligned} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{aligned}$$

It turns out that one number that solves this system of congruence equations is 23. Three more solutions are 128, 233 and 338. Notice how these numbers differ from each other by 105 which is the product of the modulus $3, 5$ and 7. This is no black magic, this is math!

Theorem 4.2. (Chinese Remainder Theorem). Let $m_1, \ldots, m_r \in \mathbb{N}$ such that they are pairwise coprime. Denote $M = \prod m_i$. Let $a_1, \ldots, a_r \in \mathbb{Z}$. Then, there exists an integer x, such that:

$$\begin{aligned} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{aligned}$$

and any two such x are congruent modulo M.

There are two main key points. The theorem asserts the **existence** of such a solution; and also that this solution is **unique** modulo M. For our first proof below, we need the following lemma first.

Lemma 4.3. (Pigenhole Principle). If A and B are finite sets such that $|A| = |B|$ and $f : A \to B$ is a map. Then, f is injective if and only if f is surjective.

The proof of this lemma is an exercise for the reader. We thus proceed to give the first proof of the Chinese Remainder Theorem.

Proof. (Mapping existence proof). Consider the map $f : \mathbb{Z}_M \to \prod_{i=1}^{r} \mathbb{Z}_{m_i}$ given by

$$x \bmod M \mapsto (x \bmod m_1, \ldots, x \bmod m_r)$$

This map maps congruence classes modulo M to sequences of congruence classes modulo m_i. We want to show this map is **bijective** – if it is injective, we get uniqueness; if it is surjective, we get existence. We first prove injectivity of this map.

Injective. Suppose that $f(x) = f(y)$, i.e. x and y both are solutions to the simultaneous congruence equations. Then $x \equiv y \bmod m_i$ for all $1 \leqslant i \leqslant r$ i.e. m_i divides $x - y$. Since m_i are pairwise coprime for all i, it follows that their product which is M divides $x - y$. Thus, we have that $x \equiv y \bmod M$. If $0 \leqslant x, y < M$, it follows that $x = y$. Thus, this map is injective.

Surjective. Note that $\mathbb{Z}_M$ and $\mathbb{Z}_{m_i}$ are both finite sets. Moreover, $|\mathbb{Z}_M| = M$ and $|\prod \mathbb{Z}_{m_i}| = \prod |\mathbb{Z}_{m_i}| = m_1 m_2 \ldots m_r = M$, so $|\mathbb{Z}_M| = |\prod \mathbb{Z}_{m_i}|$. Since $f : \mathbb{Z}_M \to \prod \mathbb{Z}_{m_i}$ is an injective map, the pigeonhole principle tells us that f is surjective. ■

We could also show injectivity by simply proving that the kernel of the map is precisely $\{0\}$. But then everything else remains quite the same.

Exercise. Prove the theorem by showing that the kernel of the map is $\{0\}$.

The proof above does not tell us anything about how the solution looks like. We give another proof that is less simple but serves as a direct construction to the solution.

Proof. (Constructive existence proof). Let $M_i = M/m_i$ be the product of all moduli except the i-th one for $1 \leqslant i \leqslant r$ i.e. $M_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_r$. Since m_i are pairwise coprime to each other, it follows that M_i and m_i are coprime. By Bezout's Lemma, there exist integers u_i, v_i such that $M_i u_i + m_i v_i = 1$. Now, the magic is to consider the following integer:

$$x = \sum_{i=1}^{r} a_i u_i M_i$$

where a_i here is the one as mentioned in the theorem's statement. This integer is in fact a solution to our simultaneous congruence equations. Let us check this. Since m_i divides M_j for $i \neq j$, it is sufficient to fix some i and see what happens in this particular case as all the other terms die anyway.

$$x = a_i u_i M_i = a_i(1 - m_i v_i) = a_i - a_i m_i v_i \equiv a_i \pmod{m_i}$$

So, it works! In fact, since i is arbitrary, this is true for all i.

Uniqueness. The uniqueness part is completely independent of the way we constructed the solution x. To see uniqueness modulo M, suppose x, y are both solutions to the simultaneous congruence equations. Then, $x - y \equiv a_i - a_i \equiv 0 \bmod m_i$ for all $1 \leqslant i \leqslant r$. So for every i, $m_i | (x - y)$. Since m_i are pairwise coprime, it follows that $M | (x - y)$ which implies $x \equiv y \bmod M$. We can go one step further and say that if

$0 \leqslant x, y < M$, then $x = y$. ■

In my opinion, this proof is better than the standard existence proof which looks at the case of two moduli and then proceed by induction. In principal, the underlying concept is the same, the way we construct the solution is also equivalent and the proof of uniqueness (as it is independent of the construction) is identical. We will abbreviate the Chinese Remainder Theorem as **CRT** from now.

Note that the construction that we have now is not very practical for hand computations. Here, we give the following trick due to Dr. Tsoi.

Lemma 4.4. (Gluing). Let p, q, r be pairwise coprime integers. The solution to the simultaneous congruence equations:

$$x \equiv a_1 \pmod{p}, \quad x \equiv a_2 \pmod{q}, \quad x \equiv a_3 \pmod{r}$$

is given by:

$$x = qr[qr]_p^{-1}a_1 + pr[pr]_q^{-1}a_2 + pq[pq]_r^{-1}a_3 \pmod{pqr}$$

where $[ij]_k^{-1}$ is the inverse of $ij \pmod{k}$.

The construction of this solution is obvious. For example, the term $qr[qr]_p^{-1}$ will die when we consider modulo p so that $qr[qr]_p^{-1}a_1 \equiv a_1 \pmod{p}$ etc. Moreover, it is not difficult to see that the Gluing Lemma can be generalized to solve more simultaneous congruence equations. We will use it now to solve Sun tzu's problem.

Example. We seek an x such that $x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}$ and $x \equiv 2 \pmod{7}$. We first compute the inverses:

$$[5 \cdot 7]_3^{-1} = 2, \quad [3 \cdot 7]_5^{-1} = 1, \quad [3 \cdot 5]_7^{-1} = 1$$

Therefore, by the CRT Trick:

$$x = (35 \cdot 2 \cdot 2) + (21 \cdot 1 \cdot 3) + (15 \cdot 1 \cdot 2) = 233 \equiv 23 \pmod{105}$$

Notice how our direct solution by the Gluing Lemma gives a number bigger than we usually want. Of course this is still a solution as we consider modulo the product of the moduli. A natural question would be, how can we make this number smaller when using the same trick. Here's how you do it.

In the Gluing Lemma, we **can only *vary* the inverse** of qr, pr and pq because these are calculated modulo p, q and r respectively. To make the final result smaller, reduce one (or two) of these inverses to negative numbers. Here we solve the same problem but we use this idea.

Example. Same Sun tzu problem. Reducing $[5 \cdot 7]_3^{-1}$ to a negative number modulo 3:

$$[5 \cdot 7]_3^{-1} = -1, \quad [3 \cdot 7]_5^{-1} = 1, \quad [3 \cdot 5]_7^{-1} = 1$$

By the Gluing lemma:

$$x = (35 \cdot (-1) \cdot 2) + (21 \cdot 1 \cdot 3) + (15 \cdot 1 \cdot 2) = 23 \pmod{105}$$

Enough of this Sun-tzu puzzle. Let's go back to why we developed this theory in the first place. We were particularly interested in the case when the modulus m is extremely large. Since we have the CRT, we can now solve the congruence $f(X) \equiv 0 \pmod{m}$ for some m large. We consider the prime factorization of m (which exists — why?). The idea

is then to solve $f(X) \equiv 0$ modulo each prime and then *glue* the solutions by CRT. This gluing process is OK since the primes are surprise surprise... pairwise coprime.

Slogan. Solve $f(X) \equiv 0$ modulo each prime and then *glue* the solutions by CRT.

Example. Find all integer solutions of $x^3 + x^2 + x \equiv 0 \pmod{105}$. Well, first let $f(X) = x^3 + x^2 + x$. Using our idea before, we solve $f(X) \equiv 0$ modulo 3, 5 and 7 separately (since $105 = 3 \cdot 5 \cdot 7$) and then glue the solutions using CRT. First, we consider **mod 3**. By the remark ($\mathbb{Z}_m$ Representations), we can choose any complete residue system of $\mathbb{Z}_3$ - for simplicity choose $\{-1, 0, 1\}$.

Mod 3.

$$\begin{aligned} f(-1) = -1 &\not\equiv 0 \pmod 3 \\ f(0) = 0 &\equiv 0 \pmod 3 \text{ 😄} \\ f(1) = 3 &\equiv 0 \pmod 3 \text{ 😄} \end{aligned}$$

Thus, $x \equiv 0, 1 \pmod 3$ are solutions.

Mod 5. Choose the complete residue system $\{-2, -1, 0, 1, 2\}$ and brute force.

$$\begin{aligned} f(-2) = -6 &\not\equiv 0 \pmod 5 \\ f(-1) = -1 &\not\equiv 0 \pmod 5 \\ f(0) = 0 &\equiv 0 \pmod 5 \text{ 😄} \\ f(1) = 3 &\not\equiv 0 \pmod 5 \\ f(2) = 14 &\not\equiv 0 \pmod 5 \end{aligned}$$

Thus, $x \equiv 0 \pmod 5$ is the only solution.

Mod 7. Choose the complete residue system $\{-3, -2, -1, 0, 1, 2, 3\}$ and brute force.

$$\begin{aligned} f(-3) = -21 &\equiv 0 \pmod 7 \text{ 😄} \\ f(-2) = -6 &\not\equiv 0 \pmod 7 \\ f(-1) = -1 &\not\equiv 0 \pmod 7 \\ f(0) = 0 &\equiv 0 \pmod 7 \text{ 😄} \\ f(1) = 3 &\not\equiv 0 \pmod 7 \\ f(2) = 14 &\equiv 0 \pmod 7 \text{ 😄} \\ f(3) = 39 &\not\equiv 0 \pmod 7 \end{aligned}$$

Thus $x \equiv -3, 0, 2 \pmod 7$ are solutions.

Gluing. To glue them, we use the Gluing Lemma. We are basically solving the simultaneous congruence equations,

$$x \equiv a_1 \pmod 3, \quad x \equiv a_2 \pmod 5, \quad x \equiv a_3 \pmod 7 \tag{4.1}$$

with $a_1 \in \{0, 1\}$, $a_2 \in \{0\}$, $a_3 \in \{-3, 0, 2\}$. Use the CRT in the spirit of the Sun tzu example to get the solutions. We expect a total of $2 \cdot 1 \cdot 3 = 6$ solutions in total. The working is left as an exercise, the solutions are:

$$x \equiv 0, 25, 30, 60, 70, 100 \pmod{105}$$

For a sanity check, take $x = 25$ and observe that:

$$f(25) = 25^3 + 25^2 + 25 = 16275 \equiv 0 \pmod{105}$$

Remark. We could have applied the Gluing Lemma to a more general setting so that we get a general form for the solutions to the simultaneous congruence equations. For example, in (4.1), we could have find the general solution using Gluing Lemma to get:

$$x \equiv 70a_1 + 21a_2 + 15a_3 \pmod{105}$$

and just plug in the values that a_1, a_2 and a_3 can take.

More examples will be added later. We will move on to discuss **inverses modulo an integer**. The question about inverses is an existence problem. Can we always find an inverses modulo an integer? Well, yes, with a caveat – what integer are we talking about here? Is it even? Odd? Prime? The safest answer to this question is – sometimes. But when can we **not** find an inverse? The following lemma will give a precise answer.

Lemma 4.5. Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. If $\gcd(a, m) = 1$, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$.

The particular b in the above lemma is called the **inverse of a modulo m**. We can take a step forward and denote the residue class $[b]_m$ to be $[a]_m^{-1}$. This is OK because, as we will see, $[b]_m$ depends only on $[a]_m$ and is independent of the choice of b. In other words, the inverse is unique modulo m.

Proof. **Existence.** Since $\gcd(a, m) = 1$, Bezout's Lemma tell us there exists x, y such that $ax + my = 1$. This is equivalent to saying $ax \equiv 1 \pmod{m}$. So the inverse exists whenever a and m are coprime.

Inverses for All. Suppose $a \equiv a' \pmod{m}$ and that x is an inverse of a modulo m. Multiplying by x we have that $ax \equiv a'x \pmod{m}$. Thus x is the inverse to a' as well i.e. we have that **if x is an inverse to $a \pmod{m}$, then x is an inverse to any integer congruent to $a \pmod{m}$.**

Uniqueness/Independence. Suppose b and b' are two inverses to $a \pmod{m}$. Then, $1 \equiv ab \equiv ab' \pmod{m}$. It follows that $m|a(b - b')$. But since $\gcd(a, m) = 1$, Euclid's Lemma tells us that $m|(b - b')$ or equivalently, $b \equiv b' \pmod{m}$ or further equivalently, $[b]_m = [b']_m$. ∎

Moreover, this lemma is a two-way street i.e. the reverse implication is true as well. This is left as an exercise, hint: use Bezout's lemma again.

Corollary 4.1. If p is prime, there exists an inverse for each $b \in \mathbb{Z}_p - \{0\}$.

Proof. If p is prime, then all elements of $\mathbb{Z}_p - \{0\}$ is coprime to p. By the previous lemma, there exist a unique inverse for each element. ∎

Could we have a nice way of rewriting the corollary above when p is not prime? Of course. But first, we have to introduce some definitions.

Definition 4.1. Define the **multiplicative group of integers modulo m** to be:

$$\mathbb{Z}_m^\times = \{[a]_m \in \mathbb{Z}_m : \gcd(a, m) = 1\}$$

Well it's no coincidence that this is called a *multiplicative group*. It satisfies all the

axioms of being a group with multiplication as defined in (3.5). This particular group is fairly interesting and will be discussed with more details in an upcoming section. To answer our short question before, we can now rewrite the previous corollary as the following.

Corollary 4.2. Let $m \in \mathbb{N}$, then there exists an inverse for each $b \in \mathbb{Z}_m^\times$.

Just as we have the notion of a *complete residue system*, we have an analogous definition for representations of $\mathbb{Z}_m^\times$.

Definition 4.2. Let $m \in \mathbb{N}$. The set $\{x_1, x_2, \ldots, x_r\}$ is called a **reduced residue system modulo** m if for all $y \in \mathbb{Z}$ with $\gcd(y, m) = 1$, there exists exactly one x_i such that $y \equiv x_i \pmod{m}$.

The ($\mathbb{Z}_m$ Representations) remark applies here also, but we will call it ($\mathbb{Z}_m^\times$ Representations) remark instead for obvious reasons. Moving on, the existence of inverses is useful to solve elementary equations modulo m.

Proposition 4.1. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. Let $d = \gcd(a, m)$. Then,

$$\exists\, x \in \mathbb{Z} \text{ such that } ax \equiv b \pmod{m} \iff d|b$$

Moreover, if $d|b$, the solutions to the congruence equation $ax \equiv b \pmod{m}$ are given by $x \in \mathbb{Z}$ with:

$$[x]_{m/d} = \left[\frac{a}{d}\right]_{m/d}^{-1} \left[\frac{b}{d}\right]_{m/d} \tag{4.2}$$

Proof. First part of the proof. ($\implies$). If $\exists\, x \in \mathbb{Z}$ such that $ax \equiv b \pmod{m}$, then $ax + mk = b$ for some $k \in \mathbb{Z}$. Since $d = \gcd(a, m)$, it follows that $d|(ax + mk) = b$.

($\impliedby$). If $d|b$, it is legal[1] to divide the equation $ax + mk = b$ by d for some $k \in \mathbb{Z}$. It follows that if $ax \equiv b \pmod{m}$, then

$$\left(\frac{a}{d}\right) x \equiv \frac{b}{d} \bmod \frac{m}{d}$$

Since $\gcd(a/d, m/d)$ is coprime, the previous lemma guarantees the existence of an inverse to a/d modulo m/d - call this $\left[\frac{a}{d}\right]_{m/d}^{-1}$. Multiplying by this inverse on both sides of the equation we have our solutions in the form as in (4.2). ∎

[1] *If you can't see it, recall that* $d = \gcd(a, m)$ *so* d *divides the LHS of the equation. If* $d|b$, d *also divides the RHS.*

4.2 Hensel's Lemma

Consider the number $L = 2,786,281,390,080,000,000,000$. This is quite a large number, there's no denying it. In words, this is 2 sextillion, 786 quintillion, 281 quadrillion, 390 trillion and 80 billion. For the engineers and the physicists, this number has an order of 21! We then pose the following question.

"*How can we find solutions to* $f(X) \equiv 0 \pmod{L}$ *for* $f \in \mathbb{Z}[X]$"

Well CRT tells us that we can deal with the equation by finding solutions modulo each prime that appears in the prime factorization of L and then glue them. Let us factorize L then, and see what appears in its prime factorization.

$$L = 2^{29} \times 3^{12} \times 5^{10}$$

Woah! We know how to solve simultaneous congruence equations modulo $2, 3$ and 5 but not their prime powers! At least not in an efficient way. If you realize, all this time, we have always been brute forcing. Before CRT we brute forced. After CRT, we factorize the modulus we are interested in and then solve the simultaneous congruence equations by brute force as well. However, it seems that brute force is not feasible anymore. You can't brute force your way to solve $x \equiv 0 \pmod{2^{29}}$. You would have to try $2^{29} = 536,870,912$ numbers! OK, the case $x = 0$ is settled. But then you still have $2^{29} - 1$ numbers to check. That is crazy to do by hand. CRT alone is not sufficient. We need a more powerful weapon. Thankfully, we have the magnificent Hensel's Lemma.

Before we give the statement of this ~~lemma~~ theorem, let's get some taste of how it works. Fix some prime number p and let $e \geqslant 1$ be an integer. Suppose x solves the congruence $f(X) \equiv 0 \pmod{(p^e)}$, then[2] x also solves $f(X) \equiv 0 \pmod{p}$. In other words, x solving $f(X) \equiv 0 \pmod{p}$ is a necessary condition for x to solve modulo p^e. Equivalently, x **not** solving modulo p implies that x **does not** solve modulo p^e. So, a natural starting point is to check whether x solves modulo p and then start to go up the exponent ladder until we reach modulo p^e. We will demonstrate this with a simple linear congruence example.

[2] If $p^e | f(X)$, then trivially $p | f(X)$. Simpler example, if $9|18$, then $3|18$.

Example. (due to Jones). We want to solve the congruence $2X \equiv 3 \bmod (5^e)$, i.e. solving $2X - 3 \equiv 0 \bmod (5^e)$. Denote $f(X) := 2X - 3$. Let's look at the case where $e = 1$.

mod 5. It is not too hard to see that the only solution of $f(X) \equiv 0 \bmod 5$ is $x \equiv 4 \bmod 5$. Let us take $x_1 = 4$ as our starting point.[3]

[3] *you could have chosen any number congruent to* 4 *modulo* 5 *as the starting point.*

mod 5^2. So, $f(x_1) = 5 = 5q_1$ where $q_1 = 1$. To solve $f(X) \equiv 0 \bmod (5^2)$, put

$$x_2 \equiv x_1 + 5k_1 \equiv 4 + 5k_1 \pmod{5^2}$$

Then, it follows that[4]

$$f(x_2) \equiv f(4 + 5k_1) \equiv 5 + 10k_1 \equiv 5q_1 + 10k_1 \pmod{5^2}$$

[4] *note that the* $q_1 = 1$ *term there is superfluous. However, it will help to understand the general pattern later as we will see.*

Thus,

$$f(x_2) \equiv 0 \pmod{5^2} \iff 2k_1 \equiv -q_1 \pmod{5}$$

we skipped some steps here, $f(x_2) \equiv 0 \pmod{5^2} \iff 10k_1 \equiv -5q_1 \pmod{5^2}$. Since $\gcd(10, 5^2) = 5$ and this divides -5, we are free to divide by 5 here.

But since $q_1 = 1$, it follows that we have the above if and only if,

$$k_1 \equiv -3 \equiv 2 \pmod{5}$$

So, $x \equiv x_2 \equiv x_1 + 5k_1 \equiv 14 \pmod{5^2}$ is the unique[5] solution to $f(X) \equiv 0 \pmod{5^2}$.

[5] *unique here means unique modulo* 5^2.

mod 5^3. We can repeat the same process. So, we have $f(x_2) = 25 = 5^2 q_2$ where $q_2 = 1$. To solve $f(X) \equiv 0 \pmod{5^3}$, put

$$x_3 \equiv x_2 + 5^2 k_2 \equiv 14 + 5^2 k_2 \pmod{5^3}$$

Then, it follows that:

$$f(x_3) \equiv f(14 + 5^2 k_2) \equiv 25 + 50k_2 \equiv 25q_2 + 50k_2 \pmod{5^3}$$

Thus,

$$f(x_3) \equiv 0 \pmod{5^3} \iff 2k_2 \equiv -q_2 \pmod{5}$$

again we have skipped some steps.

But since $q_2 = 1$, it follows that we have the above if and only if,

$$k_2 \equiv 2 \pmod{5}$$

$x_2 + 5^2 k_2 = 14 + 5^2(2 + 5k_3) = 64 + 5^3 k_3 \equiv 64 \pmod{5^3}$

So, $x \equiv x_3 \equiv x_2 + 5^2 k_2 \equiv 64 \pmod{5^3}$ is the unique solution to $f(X) \equiv 0 \pmod{5^3}$.

Note how everything looks suspiciously identical! That is because they are identical, I literally copy pasted everything and made minor edits. We can generalize this step as follows:

mod 5^e.

1. Suppose for some i, the general solution of $f(X) \equiv 0 \bmod (5^i)$ is $x \equiv x_i \bmod (5^i)$ where x_i is some integer.
2. This implies $f(x_i) \equiv 0 \bmod (5^i)$. So, $f(x_i) = 5^i q_i$ i.e. $2x_i - 3 = 5^i q_i$ for some integer q_i that we can compute directly.[6]
3. To solve $f(X) \equiv 0 \pmod{5^{i+1}}$, put $x_{i+1} \equiv x_i + 5^i k_i \bmod (5^{i+1})$ for some unknown integer k_i. Our goal is to find this k_i.
4. Now, compute $f(x_{i+1}) \equiv f(x_i + 5^i k_i) \pmod{5^{i+1}}$.
5. Then, find the restricted condition on k_i when $f(x_{i+1}) \equiv 0 \pmod{5^{i+1}}$. We then have:
$$2x_i - 3 + 2 \cdot 5^i k_i \equiv 0 \bmod (5^{i+1}) \iff 5^i q_i + 2 \cdot 5^i k_1 \equiv 0 \bmod (5^{i+1})$$
6. We can divide by $\gcd(5^i, 5^{i+1})$ to arrive at:
$$k_i \equiv 2q_i \pmod{5}$$
7. So, $x \equiv x_{i+1} \equiv x_i + 2 \cdot 5^i q_i \bmod (5^{i+1})$ is the unique solution to $f(X) \equiv 0 \bmod (5^{i+1})$.

[6] *For example, in the mod 5 case, we take* $x_1 = 4$ *and it is trivial to compute that* $q_1 = 1$.

Remark. Notice how the set of solutions *reduces* in "*size*" as we go up the exponents. In a sense, we get a restriction as the exponent gets bigger. For instance, whatever solves $f(X) \equiv 0 \bmod 5$ does not necessarily solve $f(X) \equiv 0 \bmod 5^2$. We get a restriction on what values can k_1 take. In modulo 5, k_1 can take any number on

the integer line. In modulo 5^2, k_1 can only take numbers congruent to 2 modulo 5. In modulo 5^3, $k_1 = 2 + 5k_2$, and we found that $k_2 \equiv 2 \bmod 5$, so k_1 can take numbers of the form 2 plus k_2 congruent to 2 modulo 5 etc.

The example above was linear, so we can solve it fairly easily by noticing that $3 + 5^e$ is even. Since $\gcd(2, 5^e) = 1$, we have $x \equiv (3 + 5^e)/2 \pmod{5^e}$ as the general solution. Now, we give an example to show why it would be truly wonderful if we have a shortcut to solve prime-power modulus congruences.

Example. (due to Jones). This time, we want to solve

$$f(X) = X^3 - X^2 + 4X + 1 \equiv 0 \pmod{5^e}$$

for $e = 1, 2, 3$. Let $e = 1$.

mod 5. Easy to see by inspection that $x \equiv \pm 1 \pmod 5$ solves $f(X) \equiv 0 \pmod 5$. We can start by choosing $x_1 = -1$ as our starting point.

mod 5^2. So, $f(x_1) = -5 = 5q_1$ where $q_1 = -1$. To solve $f(X) \equiv 0 \pmod{5^2}$, put

$$x_2 \equiv x_1 + 5k_1 \equiv -1 + 5k_1 \pmod{5^2}$$

Then, it follows that

$$\begin{aligned} f(x_2) &\equiv f(x_1 + 5k_1) \\ &\equiv (x_1 + 5k_1)^3 - (x_1 + 5k_1)^2 + 4(x_1 + 5k_1) + 1 \\ &\equiv \underbrace{(x_1^3 - x_1^2 + 4x_1 + 1)}_{=f(x_1)=5q_1} + \underbrace{(3x_1^2 - 2x_1 + 4)}_{=f'(x_1)=9} 5k_1 \\ &\equiv 5q_1 + 9 \cdot 5k_1 \pmod{5^2} \end{aligned}$$

we use Binomial expansion here and any term that is divisible by 5^2 dies

Thus,

$$f(x_2) \equiv 0 \pmod{5^2} \iff q_1 + 9k_1 \equiv 0 \pmod 5$$

But since $q_1 = -1$, it follows that we have the above if and only if,

$$k_1 \equiv -1 \pmod 5$$

So $x \equiv x_2 \equiv x_1 + 5k_1 \equiv -6 \pmod{5^2}$ is the unique solution to $f(X) \equiv 0 \pmod{5^2}$ **which also satisfies**[7] $x \equiv -1 \pmod 5$.

[7] *recall that we also have the case where the starting point are numbers congruent to* 1 *modulo 5.*

mod 5^3. Every process is identical, but for the sake of wanting you to see the nice pattern, we will do it – it's just copy pasting anyways. So, we have $f(x_2) = -275 = 5^2 q_2$ where $q_2 = -11$. To solve $f(X) \equiv 0 \pmod{5^3}$, put

$$x_3 \equiv x_2 + 5^2 k_2 \equiv -6 + 5^2 k_2 \pmod{5^3}$$

Then, it follows that:

$$\begin{aligned} f(x_3) &\equiv f(x_2 + 5^2 k_2) \\ &\equiv (x_2 + 5^2 k_2)^3 - (x_2 + 5^2 k_2)^2 + 4(x_2 + 5^2 k_2) + 1 \\ &\equiv \underbrace{(x_2^3 - x_2^2 + 4x_2 + 1)}_{=f(x_2)=5^2 q_2} + \underbrace{(3x_2^2 - 2x_2 + 4)}_{=f'(x_2)=124} 5^2 k_2 \\ &\equiv 5^2 q_2 + 124 \cdot 5^2 k_2 \pmod{5^3} \end{aligned}$$

we use Binomial expansion again here and any term that is divisible by 5^3 dies

Thus,

$$f(x_3) \equiv 0 \pmod{5^3} \iff 124k_2 \equiv -q_2 \pmod{5}$$

Since $q_2 = -11$, it follows that we have the above if and only if,

$$k_2 \equiv -1 \pmod{5}$$

So, $x \equiv x_3 \equiv x_2 + 5^2 k_2 \equiv -31 \pmod{5^3}$ is the unique solution to $f(X) \equiv 0 \pmod{5^3}$ **which also satisfies** $x \equiv -1 \pmod{5}$.

Before we continue and see what happens if we choose $x_1 = 1$ as the starting point, we make some remarks on these two examples so far.

Remark. Let's make some observations.

1. In both examples, in both steps we have[8] that $f(x_{i+1}) = f(x_i + 5^i k_i) = f(x_i) + f'(x_i) \cdot 5^i k_i \pmod{5^{i+1}}$ for $i = 1, 2$ where $f'(X)$ is the usual derivative of $f(X)$.
2. In both examples, we divide by 5^i to get $k_i \equiv$ something $\pmod 5$ where the coefficient of k_i is precisely $f'(x_i)$. This tells us that **we are able to solve this uniquely provided that** $f'(x_i) \not\equiv 0 \pmod 5$ (or equivalently, $f'(x_i) \not\equiv 5 \pmod 5$). To see what happens if this condition does not hold, let's go back and see what happens if we take the other solution to $f(X) \equiv 0 \pmod 5$, $x_1 = 1$ as our starting point.

[8] *in the linear congruence example, we have that the derivative was the constant 2, so it was quite implicit, hence the relevance of this non-linear example.*

Example. (continuation of the example). Choose $x_1 = 1$ as our starting point.

mod 5^2. So, $f(x_1) = 5 = 5q_1$ where $q_1 = 1$. To solve $f(X) \equiv 0 \pmod{5^2}$, put

$$x_2 \equiv x_1 + 5k_1 \equiv 1 + 5k_1 \pmod{5^2}$$

Then, it follows that

$$f(x_2) \equiv f(x_1) + f'(x_1) \cdot 5k_1 \equiv 5q_1 + 5^2 k_1 \pmod{5^2}$$

Thus,

$$f(x_2) \equiv 0 \pmod{5^2} \iff q_1 + 5k_1 \equiv 0 \pmod{5}$$

But since $q_1 = 1$, it follows that we have the above if and only if,

$$5k_1 \equiv -1 \pmod{5}$$

which is impossible as in modulo 5, 5 times anything is 0. Hence, the solution $x \equiv 1 \pmod 5$ **does not** induce any solution of $f(X) \equiv 0 \pmod 5^2$. Consequently, there is no solution modulo higher powers of 5 such that $x \equiv 1 \pmod 5$.

We will now give the statement of the theorem that will provide a shortcut to solve the example(s) above.

Theorem 4.6. (Hensel's Lemma). Let $f(X) \in \mathbb{Z}[X]$ and p a prime number. Suppose $x_r \in \mathbb{Z}_{p^r}$ satisfies the following:

$$f(x_r) \equiv 0 \pmod{p^r} \text{ and } f'(x_r) \not\equiv 0 \pmod{p}$$

Then, there exists a unique $x_{r+1} \in \mathbb{Z}_{p^{r+1}}$ such that

$$f(x_{r+1}) \equiv 0 \pmod{p^{r+1}} \text{ and } x_{r+1} \equiv x_r \pmod{p^r}$$

Moreover, the general solution is given by the lifting formula:

$$x_{r+1} \equiv x_r - f(x_r)[f'(x_r)]_p^{-1} \pmod{p^{r+1}}$$

We can even restate this theorem in a neat way. We will first give a definition.

Definition 4.3. Let $f \in \mathbb{Z}[X]$ and p a prime number. Suppose $y \in \mathbb{Z}_p$ is a root to $f(X) \equiv 0 \pmod{p^r}$ for some $r \in \mathbb{N}$. Then, y is said to be **non-simple mod p** if $f'(y) \not\equiv 0 \pmod{p}$. Otherwise, it is called **simple mod p**.

If it is clear from context that the root is non-simple modulo a certain prime, then we just say the root is **non-simple**. Otherwise, we say it is simple.

If there exists a root that is non-simple mod p, then we can basically apply Hensel's Lemma because the definition of non-simple mod p already assumed all the required assumptions for the theorem.

Theorem 4.7. (Hensel's Lemma II). Non-simple roots can be lifted uniquely.

Remark. The idea of Hensel's Lemma is the following.

1. First, you solve $f(X) \equiv 0 \pmod{p}$ and find a root $x = x_1$.
2. Then, if $f'(x_1) \not\equiv 0 \pmod{p}$, you can *lift* x_1 **uniquely** to a root of $f(X) \equiv 0 \pmod{p^n}$ for all n.
3. The root of $f(X) \equiv 0 \pmod{p^n}$ is given by the **Lifting Formula**:

$$x_n = x_{n-1} - f(x_{n-1})[f'(x_1)]_p^{-1}$$

To prove the theorem, we would need to add one weapon to our arsenal first. Recall in the example (due to Jones) where we found out that $f(x_2 + 5^2k_2) = f(x_2) + f'(x_2)5^2k_2 \pmod{5^3}$. Well the obvious question is, is this true in general? i.e. if we replace 5 by some prime p, would the identity still hold? What about if we change the index? Would this result hold if, say, $f(x_{2020} + 5^{2020}k_{2020}) = f(x_{2020}) + f'(x_{2020})5^{2020}k_{2020} \pmod{5^{2021}}$?

Lemma 4.8. Let $f \in \mathbb{Z}[X]$, $k \in \mathbb{Z}$ and fix $r \in \mathbb{N}$. Then,

$$f(X + p^r k) = f(X) + f'(X)p^r k \pmod{p^{r+1}}$$

Notice how this lemma is true for any $k \in \mathbb{Z}$.

Proof. It is sufficient to show that this is true for $g_n(X) = X^n$ where $n \in \mathbb{N}$ is arbitrary because we will write f as $f(X) = \sum c_i g_i(X)$ for some $c_i \in \mathbb{Z}$. We have:

$$g_n(X + p^r k) = (X + p^r k)^n = \sum_{i=0}^{n} \binom{n}{i} X^{n-i}(p^r k)^i$$

Now, for $i \geqslant 2$, p^{r+1} divides p^{ri} which divides $(p^r k)^i$. Thus a lot of term dies. In fact

Notice how p^{r+1} divides p^{ri} iff $r + 1 \leqslant ri \iff r(i-1) \geqslant 1$. By assumption $r \geqslant 1$. So, this is true iff $i - 1 \geqslant 1$ i.e. $i \geqslant 2$.

we have only two terms left.

$$g_n(X + p^r k) \equiv X^n + nX^{n-1}(p^r k) \pmod{p^{r+1}}$$

■

Now, we are in the position of proving Hensel's Lemma. Let us recall what we actually want to find. Given a polynomial $f \in \mathbb{Z}[X]$, we want to solve $f(X) \equiv 0 \pmod{p^{r+1}}$ for some $r \in \mathbb{N}$. Suppose we have that the solution to $f(X) \equiv 0 \pmod{p^r}$ is $x \equiv x_r \pmod{p^r}$. This has the form $x = x_r + p^r k$. Then, we ask:

"Hmm, for what k would this also be a solution to $f(X) \equiv 0 \pmod{p^{r+1}}$."

Well let's find out! Plug in this solution inside $f(X) \equiv 0 \pmod{p^{r+1}}$ to have $f(x_r+p^r k) \equiv 0 \pmod{p^{r+1}}$ and see what happens to k. This is the idea.

Slogan. Find what k such that the already root modulo p^r is also a root modulo p^{r+1}.

Proof. (Hensel's Lemma). Given that $x \equiv x_r \pmod{p^r}$ solves $f(X) \equiv 0 \pmod{p^r}$. So, p^r **divides** $f(x_r)$. To solve $f(X) \equiv 0 \pmod{p^{r+1}}$, put

$$x_{r+1} \equiv x_r + p^r k \pmod{p^{r+1}}$$

Then, it follows that

$$f(x_{r+1}) \equiv f(x_r + p^r k) \equiv f(x_r) + f'(x_r)p^r k \pmod{p^{r+1}} \tag{4.3}$$

where we used our previous lemma in the last congruence. Thus,

$$f(x_{r+1}) \equiv 0 \pmod{p^{r+1}} \iff f'(x_r)p^r k \equiv -f(x_r) \pmod{p^{r+1}}$$

Since p^r divides $f(x_r)$, **we can divide everything by p^r to get**:

$$f'(x_r)k \equiv -\frac{f(x_r)}{p^r} \pmod{p}$$

As p is prime and p **does not divide $f'(x_r)$ by hypothesis**, we have that $\gcd(f'(x_r), p) = 1$. By Lemma (4.5), there exists an inverse to $f'(x_r)$ modulo p, call this $[f'(x_1)]_p^{-1}$. So,

$$k \equiv -\frac{f(x_r)}{p^r}[f'(x_1)]_p^{-1} \pmod{p}$$

Hence, the unique solution (modulo p^{r+1}) to $f(X) \equiv 0 \pmod{p^{r+1}}$ which also satisfies $x \equiv x_r \pmod{p^r}$ is:

$$x_{r+1} \equiv x_r + p^r k \equiv x_r - f(x_r)[f'(x_1)]_p^{-1} \pmod{p^{r+1}}$$

■

To see the last congruence, plug in k to have $x_r + p^r k = x_r + p^r\left(-\frac{f(x_r)}{p^r}[f'(x_1)]_p^{-1} + p\lambda\right) \equiv x_r - f(x_r)[f'(x_1)]_p^{-1} \pmod{p^{r+1}}$ where $\lambda \in \mathbb{Z}$.

The highlighted parts are where we used all the hypothesis. In essence, what Hensel's Lemma tells us is that:

$$f'(x_1) \not\equiv 0 \pmod{p} \implies x_1 \text{ can be lifted to a root modulo } p^k \text{ , } \forall\, k$$

But the converse is **not necessarily true**, i.e. Hensel's Lemma tells us nothing if

$f'(x_1) \equiv 0 \pmod{p}$.

Remark. Here, we highlight some things regarding Hensel's Lemma.

1. The prime can be 2.
2. You don't necessarily need to start from the case exponent $= 1$.
3. You can lift as many times as you like.
4. A root modulo p^{r+1} is also a root modulo p^r but the other way around is not always true. This is where the term *lifts* come from. You try to lift a root modulo p^r to become a root modulo p^{r+1}.
5. Since $p \mid p^r$ and the new root $x_{r+1} \equiv x_r \pmod{p^r}$ i.e. $p^r \mid (x_{r+1} - x_r)$, thus $x_{r+1} \equiv x_r \pmod{p}$. Hence, the new root would satisfy the condition $f'(x_{r+1}) \equiv f'(x_r) \not\equiv 0 \pmod{p}$. **Therefore, we can lift indefinitely!**
6. If p^{r+1} divides $f'(x_r)$, then p divides $f'(x_r)$ by transitivity. In other words, if p does not divide $f'(x_r)$, then p^{r+1} does not divide $f'(x_r)$ i.e.

$$f'(x_r) \not\equiv 0 \pmod{p} \implies f'(x_r) \not\equiv 0 \pmod{p^{r+1}}$$

   This explains why we need to check the condition that $f'(x_r) \not\equiv 0 \pmod{p}$ only once at exponent $= 1$.
7. If $f'(x_1) \equiv 0 \pmod{p}$, we cannot use Hensel's Lemma. **It does not mean that there are no solutions modulo higher powers**. This is further explained in a remark below.
8. Since the lifts are unique, if there are k solutions to $f(X) \equiv 0 \pmod{p^r}$ and **all are non-simple** mod p^r, then there are precisely k solutions to $f(X) \equiv 0 \pmod{p^{r+1}}$.

note the word **all**. If say there are 5 solutions to the $f(X) \equiv 0 \pmod{p^r}$ and only 3 are non-simple, then there are precisely 3 solutions to $f(X) \equiv 0 \pmod{p^{r+1}}$.

Let us look at one example.

Example. **Find all the solutions to** $f(X) \equiv X^4 - 1 \equiv 0 \pmod{25}$. We begin by first noticing that $25 = 5^2$ and stating $f'(X) = 4X^3$. So, we first solve $X^4 - 1 \equiv 0 \pmod{5}$. By Fermat's Little Theorem (cf. Corollary (5.4)) , $X \equiv 1, 2, 3, 4 \pmod{5}$ are roots. Let us check which roots are non-simple.

$$\begin{aligned} f'(1) &\equiv 4(1)^3 \equiv 4 \not\equiv 0 \pmod{5} \\ f'(2) &\equiv 4(2)^3 \equiv 2 \not\equiv 0 \pmod{5} \\ f'(3) &\equiv 4(3)^3 \equiv 3 \not\equiv 0 \pmod{5} \\ f'(4) &\equiv 4(4)^3 \equiv 1 \not\equiv 0 \pmod{5} \end{aligned}$$

So, all the roots are non-simple. By Hensel's Lemma, we can lift them uniquely to a root of mod 5^2. We use the lifting formula $x_2 \equiv x_1 - f(x_1)[f'(x_1)]_5^{-1} \pmod{5^2}$ to get

$$\begin{aligned} a &\equiv 1 - f(1)[f'(1)]_5^{-1} \equiv 1 \pmod{5^2} \\ b &\equiv 2 - f(2)[f'(2)]_5^{-1} \equiv 2 - 15 \cdot 3 \equiv -43 \equiv 7 \pmod{5^2} \\ c &\equiv 3 - f(3)[f'(3)]_5^{-1} \equiv 3 - 80 \cdot 2 \equiv -157 \equiv 18 \pmod{5^2} \\ d &\equiv 4 - f(4)[f'(4)]_5^{-1} \equiv 4 - 255 \cdot 1 \equiv -251 \equiv 24 \pmod{5^2} \end{aligned}$$

So $a \equiv 1 \pmod{5^2}$, $b \equiv 7 \pmod{5^2}$, $c \equiv 18 \pmod{5^2}$ and $d \equiv 24 \pmod{5^2}$ are the solutions to $f(X) \equiv 0 \pmod{5^2}$.

Exercise. Verify all the solutions by hand or software — Python or Mathematica maybe?

Remark. Going back to the theorem, what is interesting now is to see what happens if $f'(x_r) \equiv 0 \pmod{p}$. We go back and see (4.3). In fact, we will restate it here.

$$f(x_{r+1}) \equiv f(x_r + p^r k) \equiv f(x_r) + f'(x_r)p^r k \pmod{p^{r+1}}$$

Since $p | f'(x_r)$, we can write $f'(x_r) = p\lambda$ for some $\lambda \in \mathbb{Z}$. It follows that the red term above becomes $p^{r+1}\lambda k$ and this is divisible by p^{r+1} so it dies.

This equation now reduces to $f(x_r + p^r k) \equiv f(x_r) \pmod{p^{r+1}}$ for any $k \in \mathbb{Z}$. Consequently, we could only have the following two cases:

1. $f(x_r) \equiv 0 \pmod{p^{r+1}} \implies f(x_r + p^r k) \equiv 0 \pmod{p^{r+1}}$. So, every lifting of x_r to modulus p^{r+1} is a root[9] of $f(X)$ modulo p^{r+1}.
2. $f(x_r) \not\equiv 0 \pmod{p^{r+1}} \implies f(x_r + p^r k) \not\equiv 0 \pmod{p^{r+1}}$. Unfortunately, this just means there is no lifting[10] of x_r to a root of $f(X)$ modulo p^{r+1}.

If the implications of the condition on lifting above is not clear, you might want to reread the proof or the example(s) above. Oh! Maybe just go and reread the slogan.

[9] *In other words, there is* ***no restriction*** *on the k that we are trying to find.*

[10] *In other words, there is* ***full restriction*** *on the k that we are trying to find.*

Our final remark on Hensel's Lemma basically is the proof of the following corollary.

Corollary 4.3. If $x \in \mathbb{Z}$ is a simple root mod p, then either every lifting of x to modulus p^r (where $r \in \mathbb{N}$) is a root or there is no lifting at all.

Example. Let $f(X) = X^3 + 3X + 5$ and suppose we want to solve $f(X) \equiv 0 \pmod{9}$. We solve $f(X) = 0 \pmod{3}$ first. By brute-force, clearly $x_1 = 1$ is the only solution. Now $f'(X) = 3X^2 + 3 \equiv 0 \pmod{3}$, and so $f'(x_1) \equiv 0 \pmod{3}$ i.e. x_1 is a simple root mod 3. By the preceding corollary, either every lifting of x_1 to modulus $3^2 = 9$ is a root or there is no lifting at all. But then obviously, $f(x_1) \equiv 0 \pmod{9}$. So there is one lift, and thus every lifting of x_1 is a root. What are the other lifts? Well since $x_1 \equiv 1 \pmod{3}$ solves $f(X) \equiv 0 \pmod{3}$, we can write $x_1 = 1 + 3k$ for some $k \in \mathbb{Z}$. The only k that makes x_1 non-repetitive modulo 9 are $k = 0, 1, 2$ and so $x_2 = 1, 4, 7$ are all the roots (lifted from x_1) to $f(X) = 0 \pmod{9}$.

4.3 Lagrange's Theorem

Now, we have a complete set of tools to tackle any congruence equation problem. Let us now state the final theorem of this section which allow us to have some control on the number of admissible solutions to congruence equations modulo p, a prime.

Theorem 4.9. (**Lagrange's Theorem**). Let p be a prime and $f \in \mathbb{Z}[X]$ such that $\deg(f) = n$ where $n \geqslant 1$. Then, $f(X) \equiv 0 \pmod{p}$ has at most n solutions in $\mathbb{Z}_p$.

This theorem will also be referred to as *Lagrange's Theorem on polynomials* or *Polynomial roots mod p Theorem* in this text. This is to avoid confusion with the more well known Lagrange's Theorem of finite groups which will appear in an upcoming section. To prove this theorem, we would first need the following lemma.

Lemma 4.10. Let $a \in \mathbb{Z}$. Then, for any non-negative integer i, $x - a$ divides $x^i - a^i$.

Proof.

$$x^i - a^i = (x - a)(x^{i-1} + ax^{i-2} + \cdots + a^{i-2}x + a^{i-1}) \tag{4.4}$$

■

Remark. The above lemma does not need that a is an integer root to some polynomial. This is an identity, expand out the parentheses if you are not convinced.

The following proof is non-examinable for the course, but it is not too hard, just a bit tedious so we will still give it.

Proof. We prove by induction on n.

Base Case. The base case $n = 1$ is a linear congruence, we know how to solve this, and we know we can only get 1 or 0 solution modulo p.

Inductive Step. Suppose the conclusion is true for polynomials up to degree $n = k - 1$ i.e. if $f \in \mathbb{Z}[X]$ such that $\deg(f) = k - 1$, then $f(X) \equiv 0 \pmod{p}$ has at most $k - 1$ solutions in $\mathbb{Z}_p$.

k-th step. Let $f \in \mathbb{Z}[X]$ such that $\deg(f) = k$. If there are no solutions to $f(X) \equiv 0 \pmod{p}$, then we are done. So, suppose there is a solution $\lambda \in \mathbb{Z}$. Thus, $f(\lambda) \equiv 0 \pmod{p}$. At the moment, f has only one solution. We have

$$\begin{aligned} f(X) &\equiv f(X) - 0 \pmod{p} \\ &\equiv f(X) - f(\lambda) \pmod{p} \\ &\equiv \sum_{i=0}^{k} c_i X^i - \sum_{i=0}^{k} c_i \lambda^i \pmod{p} \\ &\equiv \sum_{i=0}^{k} c_i (X^i - \lambda^i) \pmod{p} \end{aligned}$$

By Lemma (4.10), $(X - \lambda)$ divides $X^i - \lambda^i$ for all $0 \leqslant i \leqslant k$, so it divides their linear combination. Thus, we can rewrite the funny sum above to be

$$f(X) \equiv (X - \lambda)g(X) \pmod{p}$$

where $g(X)$ is a polynomial with integer coefficients of degree $k-1$. By the **inductive**

hypothesis, $g(X)$ has at most $k-1$ solutions. Now suppose ω is another solution. Then, $f(\omega) \equiv 0 \pmod{p}$. We have

$$0 \equiv f(\omega) \equiv (\omega - \lambda)g(\omega) \pmod{p}$$

So, $p|(\omega-\lambda)g(\omega)$. **But p is prime**, so either p divides $\omega - \lambda$ or p divides $g(\omega)$ i.e. we have

$$\omega \equiv \lambda \pmod{p} \text{ or } g(\omega) \equiv 0 \pmod{p}$$

What can we conclude? Well we have shown that **(i)** any other solution ω is congruent to our first root λ modulo p – this counts as 1 solution; and **(ii)** any other solution of f gives a solution of g modulo p. Since g has at most $k-1$ solutions (modulo p) by the inductive hypothesis, it follows that in total f can has at most $1+(k-1) = k$ solutions modulo p — either the one which is congruent to our initial assumed solution, λ modulo p or one of the $k-1$ residue classes (different from λ) that solves $g(X) \equiv 0 \pmod{p}$. ■

Remark. We really need p to be prime here.

Example. Non-example really. Consider $x^2 \equiv 1 \pmod{8}$. This has solutions $x \equiv 1, 3, 5, 7 \pmod{8}$ so there are more than 2 solutions modulo 8.

If you can't wrap your head around the conclusion of the proof above. Let's think about an example where we follow the step of the proof (almost exactly).

Example. Consider $f(X) \equiv X^3 + X^2 + X - 3$ and we want to find a root of this mod 11 i.e. we want to solve $f(X) \equiv 0 \pmod{11}$. With a bit of computation, we can find that $x \equiv 1, 2, 7 \bmod 11$ are solutions to this equation. Suppose we take $x = 1$ (was λ in the proof) as our first solution.

$$\begin{aligned} f(X) &\equiv f(X) - 0 \pmod{11} \\ &\equiv f(X) - f(1) \pmod{11} \\ &\equiv X^3 + X^2 + X - 3 - (1^3 + 1^2 + 1 - 3) \pmod{11} \\ &\equiv (X^3 - 1^3) + (X^2 - 1^2) + (X - 1) + (-3 + 3) \pmod{11} \end{aligned}$$

By Lemma (4.10), $(X-1)$ divides $(X^i - 1^i)$ for all $0 \leqslant i \leqslant 3$. Instead of just writing $g(X)$ as in the proof, we will write explicitly what $g(X)$ looks like here. We have

$$f(X) \equiv (X-1)\underbrace{\{(X^2 + X + 1^2) + (X+1) + 1 + 0\}}_{=g(X)} \pmod{11}$$

Simplifying, we have $g(X) = X^2 + 2X + 3$. Now, we have two + one cases.

Case 1 — $\omega \equiv \lambda \pmod{p}$. Let's see what happens if we take another solution that is congruent to 1 modulo 11. Take, say, 12.

$$0 \equiv f(12) \equiv (12-1)(12^2 + 2 \cdot 12 + 3) \pmod{11}$$

It couldn't be more obvious that in this case, $p = 11$ divides $(12-1) = 11$. So, we still have only one solution here, the same solution, the residue class $[1]_{11}$. This is the case where we concluded $\omega \equiv \lambda \pmod{p}$ in the proof.

Case 2 — $g(\omega) \equiv 0 \pmod{p}$ I. Now suppose, we take another solution not congruent

to 1 modulo 11, say, $x = 2$. Then

$$0 \equiv f(2) \equiv (2-1)(2^2 + 2 \cdot 2 + 3) \pmod{11}$$

Clearly, 11 does not divide $2 - 1 = 1$, but 11 divides $(2^2 + 2 \cdot 2 + 3) = 11$. So, the solution $[2]_{11}$ of $f(X) \equiv 0 \pmod{11}$ gives a solution to $g(X) \equiv 0 \pmod{11}$. This is the case where we concluded $g(\omega) \equiv 0 \pmod{p}$ in the proof.

Case 3 — $g(\omega) \equiv 0 \pmod{p}$ II. Suppose we take the other solution not congruent to 1 modulo 11, that is $x = 7$. Then

$$0 \equiv f(7) \equiv (7-1)(7^2 + 2 \cdot 7 + 3) \pmod{11}$$

Again, very obvious that 11 does not divide $7-1 = 6$, but 11 divides $(7^2+2\cdot7+3) = 66$. So the solution $[7]_{11}$ of $f(X) \equiv 0 \pmod{11}$ gives a solution to $g(X) \equiv 0 \pmod{11}$, but this one is different from $[2]_{11}$.

Conclusion. Indeed, $g(X) \equiv 0$ has 2 solutions modulo 11, $[2]_{11}$ and $[7]_{11}$ (in fact by the theorem, we now know these are all the solutions) and these 2 are different from $[1]_{11}$ which only solves $f(X) \equiv 0$ and not $g(X) \equiv 0$ modulo 11. So, in total $f(X)$ has $1+2 = 3$ roots which is the most it can take by the theorem above (since $\deg(f) = 3$).

This example is really going backwards rather than forward in view of the theorem. It is given so that you can get a good feel of why the theorem works and why the proof is correct. Here, we know the solutions beforehand because the equation can be solved fairly easily. But practically, when we start solving a congruence equation, we don't really know which ones are the solution(s). Thankfully, Lagrange's Theorem are able to tell us how many solutions we should expect.

5 Euler's Totient Function

Recall how we defined the multiplicative group of integers modulo m, $\mathbb{Z}_m^\times$ in (4.1).

Definition 5.1. Let $m \in \mathbb{N}$. We define the **Euler's totient function** (or Euler's ϕ function) to be the cardinality of $\mathbb{Z}_m^\times$. We write this as $\phi(m) = |\mathbb{Z}_m^\times|$.

Example. If p is prime, $\phi(p) = |\mathbb{Z}_p^\times| = p - 1$.

Remark. By definition of $\mathbb{Z}_m^\times$, $\phi(m) = \#\{a \in \mathbb{Z} : 1 \leqslant a \leqslant m \text{ and } \gcd(a, m) = 1\}$

Remark. There is exactly one integer between 1 and 1 such that $\gcd(1, 1) = 1$ which is just $[1]_1$. So, $\phi(1) = 1$.

Definition 5.2. An **arithmetic function** is a real- or complex-valued function defined on $\mathbb{N}$ i.e. a map $f : \mathbb{N} \to \mathbb{R}$ or $\mathbb{C}$.

Definition 5.3. We say that an arithmetic function f is **multiplicative** if $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

Definition 5.4. We say that an arithmetic function f is **completely multiplicative** if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

Here, we give our first statement of this section.

Lemma 5.1. Let $a \in \mathbb{Z}$ and $m, n \in \mathbb{N}$. Then

$$\gcd(a, mn) = 1 \iff \gcd(a, m) = \gcd(a, n) = 1$$

This lemma would or would not be useful depending on how we prove the next theorem. We will give the proof anyway as we think it is just good for general knowledge.

Proof. ($\implies$). Suppose $\gcd(a, mn) = 1$ i.e. a and mn are coprime. Notice that any common divisor of a and m must be a common divisor of a and mn. Thus[11], if $\gcd(a, mn) = 1$, we have $\gcd(a, m) = 1$. By a similar argument, we must also have $\gcd(a, n) = 1$.

($\impliedby$). Suppose $\gcd(a, m) = \gcd(a, n) = 1$. Assume for the sake of contradiction that $\gcd(a, mn) = d$ where $d \neq 1$. By the Fundamental Theorem of Arithmetic, there exists a prime p such that $p \mid d$. Since, $d \mid mn$, it follows that $p \mid mn$ by transitivity. By Euclid's Lemma, $p \mid m$ or $p \mid n$. But note that $p \mid d$ also implies $p \mid a$ as $d|a$ [↯]. ■

[11] *if you can't see this, think Bezout's lemma.*

We could have given a simpler proof for the ($\impliedby$) case but this requires Lemma (1.4) which requires m, n to be coprime. Of course proving the case which restricts m, n to be coprime is sufficient to prove the next theorem. However, this generalized version is much more useful in my opinion.

Exercise. Prove the previous lemma in a different way. Hint: Use Bezout's lemma for both if, and only if.

5.1 Multiplicativity of totient function

Theorem 5.2. Let $m, n \in \mathbb{N}$ be coprime. Then, there is a bijection:

$$\mathbb{Z}_{mn}^{\times} \to \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$$

We give the first proof of the theorem which relies on the previous lemma.

Proof. Recall that CRT gives a bijection $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ i.e. it maps $x \bmod (mn)$ to the sequence $(x \bmod m, x \bmod n)$. By the previous lemma, we then know it maps units $u \bmod (mn)$ to pair of units $(u \bmod m, u \bmod n)$. Since this map is a bijection, every pair of units is the image of ~~some~~ a unit $u \bmod (mn)$. In other words, the bijection given by the CRT restricts to a bijection $\mathbb{Z}_{mn}^{\times} \to \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$. ■

Exercise. Explain why did we cross "*some*" and put "a" instead.

Notice that the bijection that we used here is not at all new. In fact, it is just the bijection given by CRT. Of course it is not at all obvious before we had Lemma (5.1). For whatever its worth, we will still mention a slogan for this theorem.

Slogan. The bijection mapping units to pair of units is just the bijection given by CRT restricted to units.

An alternative proof to this theorem requires some knowledge on ring theory. Denote $\cong$ to mean an isomorphism (of rings or groups). Let R, S be rings. Then we have

1. $R \cong S \implies R^{\times} \cong S^{\times}$
2. $(R \times S)^{\times} \cong R^{\times} \times S^{\times}$

Proof. Since the CRT actually gives an isomorphism of rings $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n.$, i.e. we have $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Then

$$(\mathbb{Z}_{mn})^{\times} \cong (\mathbb{Z}_m \times \mathbb{Z}_n)^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$$

where we have used the first fact of general rings in the first isomorphism and the second fact on the second isomoprhism. ■

It looks simple because we didn't do the dirty work of proving the first and second fact that we stated above.

Exercise. Give a different proof to Theorem (5.2), arguing only using pure number theory.

Corollary 5.1. ϕ is multiplicative i.e. $\phi(mn) = \phi(m)\phi(n)$ whenever $\gcd(m, n) = 1$.

Proof.

$$\phi(mn) = |\mathbb{Z}_{mn}^{\times}| = |\mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}| = |\mathbb{Z}_m^{\times}||\mathbb{Z}_n^{\times}| = \phi(m)\phi(n)$$

We have the second equality because we have shown that there is a bijection (the bijection given by CRT restricted to units). ■

Remember that m and n must be coprime! When the coprimality assumption is violated, the result may not hold. This is because it relies on Theorem (5.2) which requires m, n to be coprime and this theorem relies on the Chinese Remainder Theorem which requires m, n to be coprime.

Remark. We can extend this result and say, if $m_1, m_2, \ldots, m_k$ are all pairwise coprime, then:

$$\phi(m_1 m_2 \dots m_k) = \phi(m_1)\phi(m_2)\dots\phi(m_k)$$

This is done by iteration, so we truly need that they are **pairwise** coprime.

Remark. Another way to see that $\phi(1) = 1$ is using this corollary. Since $\gcd(1,1) = 1$, $\phi(1) = \phi(1)\phi(1)$. It follows that $\phi(1) = 1$.

Exercise. Justify the fact that we can divide by $\phi(1)$ on both sides in the remark above.

Example. $\phi(9) = 6 \neq 4 = \phi(3)\phi(3)$

5.2 Generalizing the totient function

Now consider the number 5, then

$$\phi(3) = 2$$

How about $\phi(5^2)$? Well, the example above shows we can't directly use multiplicativity of $\phi(\cdot)$ to compute this. Thankfully, we know how to count. We get

$$\phi(5^2) = \phi(25) = \#\{a \in \mathbb{Z} : 1 \leqslant a \leqslant 25 \text{ and } \gcd(a, 25) = 1\} = |\mathbb{Z}_{25}^{\times}| = 20$$

How about $\phi(3^3)$? We can count this also:

$$\phi(5^3) = \phi(125) = \#\{a \in \mathbb{Z} : 1 \leqslant a \leqslant 125 \text{ and } \gcd(a, 125) = 1\} = |\mathbb{Z}_{125}^{\times}| = 100$$

Clearly, this process is not iterative as counting $|\mathbb{Z}_{25}^{\times}|$ does not affect counting $|\mathbb{Z}_{125}^{\times}|$ or even counting $|\mathbb{Z}_{3125}^{\times}|$ where $3125 = 5^5$. Our aim now is to find a generalized formula to compute $\phi(p^k)$ for p prime and $k \in \mathbb{N}$.

Let us take things slowly and think again what is $\phi(5^2)$. Again, we have:

$$\begin{aligned}\phi(5^2) &= \#\{a \in \mathbb{Z} : 1 \leqslant a \leqslant 25 \text{ and } \gcd(a, 25) = 1\} \\ &= \text{ number of integers between 1 and 25 which are coprime to 25}\end{aligned}$$

Now, $25 = 5^2$, so by Lemma (5.1), being coprime to 25 is equivalent to being coprime to 5 i.e. not being divisible by 5. Let us write down a complete residue system modulo 25.

	1	2	3	4	**5**
	6	7	8	9	**10**
	11	12	13	14	**15**
	16	17	18	19	**20**
	21	22	23	24	**25**

Notice how the **red-bolded** numbers are all the numbers in the complete residue system modulo 25 which are divisible by 5. We don't want them, so we cross them out.

	1	2	3	4	~~5~~
	6	7	8	9	~~10~~
	11	12	13	14	~~15~~
	16	17	18	19	~~20~~
	21	22	23	24	~~25~~

What's left is now a reduced residue system modulo 25 i.e. a complete set of representations for $\mathbb{Z}_{25}^{\times}$. How many elements are there? Well, there are precisely $5 \times 4 = 20$ elements which is $\phi(5^2)$. How about $\phi(5^3)$?

$$\begin{aligned}\phi(5^3) &= \#\{a \in \mathbb{Z} : 1 \leqslant a \leqslant 5^3 \text{ and } \gcd(a, 5^3) = 1\} \\ &= \text{number of integers between 1 and } 5^3 \text{ which are coprime to } 5^3 \\ &= \text{number of integers between 1 and } 5^3 \text{ which are coprime to } 5\end{aligned}$$

Writing down a complete residue system modulo 5^3.

It may seem superfluous to write down this many elements in the table. However, it is there to remind you how large the rows can get when generalizing this idea later.

	1	2	3	4	**5**
	6	7	8	9	**10**
	11	12	13	14	**15**
	16	17	18	19	**20**
	21	22	23	24	**25**
	26	27	28	29	**30**
	31	32	33	34	**35**
	36	37	38	39	**40**
	41	42	43	44	**45**
	46	47	48	49	**50**
	51	52	53	54	**55**
	56	57	58	59	**60**
	⋮	⋮	⋮	⋮	⋮
	⋮	⋮	⋮	⋮	⋮
	⋮	⋮	⋮	⋮	⋮
	116	117	118	119	**120**
	121	122	123	124	**125**

This is a 25 (rows) $\times$ 5 (columns) table. We don't want the **red-bolded** numbers so we delete the last column. Now we have only 4 columns left. What's left on the table is a reduced residue system modulo 125 i.e. a complete set of representations for $\mathbb{Z}_{125}^{\times}$. How many elements are there now? There are $\phi(5^3) = 25 \times 4 = 120$ elements.

Let's generalize this for any prime number p. What is $\phi(p^2)$?

$$\begin{aligned}\phi(p^2) &= \#\{a \in \mathbb{Z} : 1 \leqslant a \leqslant p^2 \text{ and } \gcd(a, p^2) = 1\} \\ &= \text{number of integers between 1 and } p^2 \text{ which are coprime to } p^2 \\ &= \text{number of integers between 1 and } p^2 \text{ which are coprime to } p\end{aligned}$$

Let us write down a complete residue system modulo p^2.

$$\begin{array}{|llll|l}
1 & 2 & \cdots & \cdots & p \\
p+1 & p+2 & \cdots & \cdots & 2p \\
\vdots & \vdots & \ddots & & \vdots \\
p(p-2)+1 & p(p-2)+2 & & \ddots & p(p-1) \\
p(p-1)+2 & p(p-1)+2 & \cdots & \cdots & p^2
\end{array}$$

This is a $p \times p$ table i.e. it has p^2 elements. Again notice that the **red-bolded** numbers are all the numbers in the complete residue system modulo p^2 which are divisible by p. So we can delete that last column to get a complete set of representations for $\mathbb{Z}_{p^2}^{\times}$. How many elements are there? There are precisely $\phi(p^2) = p(p-1)$ elements.

How about $\phi(p^3)$? Well, use the same argument, but now we need to extend the table.

$$\begin{array}{|llll|l}
1 & 2 & \cdots & \cdots & p \\
p+1 & p+2 & \cdots & \cdots & 2p \\
\vdots & \vdots & \ddots & & \vdots \\
p(p-2)+1 & p(p-2)+2 & & \ddots & p(p-1) \\
p(p-1)+2 & p(p-1)+2 & \cdots & \cdots & p^2 \\
p^2+1 & p^2+2 & \cdots & \cdots & 2p^2 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
p^2(p-2)+1 & p^2(p-2)+2 & & \ddots & p^2(p-1) \\
p^2(p-1)+1 & p^2(p-1)+2 & \cdots & \cdots & p^3
\end{array}$$

This is a p^2 (rows) $\times$ p (columns) table i.e. it has p^3 elements. Deleting the last column, we are left with $p-1$ columns. How many elements are there here? There are exactly $\phi(p^3) = p^2(p-1)$ elements. Notice how by this construction, we always have p columns. So, upon deletion of the last column, we will always end up with $p-1$ columns. The only one that is varying is the rows which depends on our choice.

Slogan. Get p^{k-1} (rows) $\times$ p (columns) table of integers, then delete the last column. The number of elements in this new table is $\phi(p^k)$.

We can generalize this easily now.

Proposition 5.1. Let p be a prime and $k \in \mathbb{N}$. Then,

$$\phi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$$

Although we have write this again and again, we will put it here because this fact will be useful to follow the proof.

$$\begin{aligned}
\phi(p^k) &= \#\{a \in \mathbb{Z} : 1 \leqslant a \leqslant p^k \text{ and } \gcd(a, p^k) = 1\} \\
&= \text{ number of integers between 1 and } p^k \text{ which are coprime to } p^k \\
&= \text{ number of integers between 1 and } p^k \text{ which are coprime to } p
\end{aligned}$$

Proof. Let $1 \leqslant a \leqslant p^k$. Since p is prime, $\gcd(p^k, a)$ can only be one of $\{1, p, p^2, \ldots, p^k\}$. The only way for $\gcd(p^k, a) \neq 1$ i.e. a **and** p^k **are not coprime**, is if that p divides a. But $1 \leqslant a \leqslant p^k$. The only number that p divides in this range are $\{p, 2p, 3p, \ldots, p^{k-2}p, p^k\}$ and there are precisely p^{k-1} of them. Thus, $p^k - p^{k-1}$ are those which a **and** p^k **are coprime**. By definition, this is $\phi(p^k)$. ■

A more compact version of this proof is given below:

Proof. Compact Version. Let $1 \leqslant a \leqslant p^k$. Then $\gcd(a, p^k) = 1$ if and only if p does not divide a. All the numbers in the range $1, 2, \ldots, p^k$ are coprime to p^k except $p, 2p, 3p, \ldots, p^{k-1}p = p^k$. Thus, $\phi(p^k) = p^k - p^{k-1}$. The result follows. ■

If you are not convinced, you can look at a specific case, for example take $p = 3$. We now have this tool to compute even ridiculous values like $\phi(500) = \phi(2^2 \cdot 5^3) = \phi(2^2)\phi(5^3) = 2 \cdot 5^2(4) = 200$.

Proposition 5.2. If $m \geqslant 3$, then $\phi(m)$ is even. Moreover, if m has k distinct odd prime factors, then $2^k \mid \phi(m)$.

Proof. Suppose that $\phi(m)$ is odd for $m \geqslant 3$. By the Fundamental Theorem of Arithmetic, write $m = \prod_{i=1}^{k} p_i^{a_i}$ for some p_i distinct primes and $a_i \in \mathbb{N} \cup \{0\}$ for all $1 \leqslant i \leqslant k$. Then,

$$\phi(m) = \phi\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} \phi(p_i^{a_i}) = \prod_{i=1}^{k} (p_i^{a_i - 1})(p_i - 1) \qquad (*)$$

If just one p_i is odd, then $p_i - 1$ is even which would imply $\phi(m)$ to be even, contradiction! So, suppose p_i is even for all i. This just means m is a power of 2. Write this as $m = 2^j$ for some $j \geqslant 2$ (as $m \neq 1, 2$ by hypothesis). Now

$$\phi(m) = \phi(2^j) = 2^{j-1}$$

But then 2^{j-1} is odd if and only if $j - 1 = 0$ i.e. $j = 1$. [↯]. The first part of the claim follows.

Moreover, from $(*)$ we can see that each odd prime gives a factor of 2 (from $p_i - 1$). There are k distinct odd primes so they altogether gives a factor of 2^k. The second part of the claim follows. ■

Theorem 5.3. Let $n \in \mathbb{N}$ and p be a prime number. Then

$$\phi(pn) = p\phi(n) \iff p \text{ divides } n.$$

Proof. Let $n = p^\alpha m$ for some $\alpha \in \mathbb{N} \cup \{0\}$ and such that $\gcd(p, m) = 1$. Then observe that

if $\gcd(p, m) = 1$, then $\gcd(p^\alpha, m) = 1$ for any $\alpha > 0$.

$$\phi(pn) = \phi(p^{\alpha+1}m) = \phi(p^{\alpha+1})\phi(m).$$

Also, we compute:

$$p\phi(n) = p\phi(p^\alpha m) = p\phi(p^\alpha)\phi(m).$$

Finally, we make the observation that:

$$\phi(pn) = p\phi(n) \iff \phi(p^{\alpha+1}) = p\phi(p^\alpha) \iff \alpha > 0 \iff p|n.$$

as desired. ∎

We have a generalization of this theorem. But first we will need the following lemma.

Lemma 5.4. Let $n = \prod_{i=1}^{r} p_i^{a_i}$ where p_i are distinct primes and $a_i \in \mathbb{N} \cup \{0\}$ for all $1 \leqslant i \leqslant r$. Then

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

N.B. this does not mean that $n|\phi(n)$ as the product is not an integer!

Proof.

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{a_i}) = \prod_{i=1}^{r} p_i^{a_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{r} p_i^{a_i} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

∎

Remark. Using a slightly different notation, we can write this as

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Theorem 5.5. Let $d = \gcd(m, n)$ Then,

$$\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)}$$

Proof. By the preceding lemma, we have

$$\phi(mn) = mn \prod_{p|mn} \left(1 - \frac{1}{p}\right) = mn \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|d} \left(1 - \frac{1}{p}\right)} = \phi(m)\phi(n)\frac{d}{\phi(d)}.$$

∎

Corollary 5.2. $a \mid b$ implies $\phi(a) \mid \phi(b)$.

Proof. Since $a \mid b$, we have $b = ak$ where $1 \leqslant k \leqslant b$. If $k = b$, then $a = 1$ and the result holds. Suppose $k < b$. By the preceding theorem, we have

$$\phi(b) = \phi(ak) = \phi(a)\phi(k)\frac{d}{\phi(d)} = d\phi(a)\frac{\phi(k)}{\phi(d)} \qquad (*)$$

where $d = \gcd(a, k)$. Then the result follows by induction on b.

If $b = 1$, the result holds trivially. Suppose that the result is true for all integers less than b. Then it holds for k (as $k < b$) so $\phi(d) \mid \phi(c)$ since $d \mid c$. Hence the far-most RHS of $(*)$ is a multiple of $\phi(a)$ i.e. $\phi(a) \mid \phi(b)$, as desired. ∎

Proposition 5.3. Let $n > 1$ and let $a_1, a_2, \ldots a_{\phi(n)}$ be the positive integers less than n and coprime to n. Then

$$\sum_{i=1}^{\phi(n)} a_i = \sum_{i=1}^{\phi(n)} (n - a_i).$$

it doesn't matter to say "less than" or "less than or equal to" here as the positive integers less than n **and** coprime to n can't strictly be n itself as $\gcd(n, n) = n$.

Proof. We use a counting argument. If we consider $n - a_i$ for $i \in \{1, 2, \ldots, \phi(n)\}$, then we have $\phi(n)$ distinct positive integers which are less than n and coprime to n. This means that the list $n - a_1, \ldots, n - a_{\phi(n)}$ is the same list as $a_1, \ldots, a_{\phi(n)}$ but in reverse order. So their sum must be equal. ■

Corollary 5.3. Let $n > 1$. Then the number of positive integers less than n and coprime to n is precisely $\frac{1}{2}n\phi(n)$.

Proof. Let $S := \sum_{i=1}^{\phi(n)} a_i$. Now observe that

$$S' = \sum_{i=1}^{\phi(n)} (n - a_i) = n\phi(n) - \sum_{i=1}^{\phi(n)} a_i = n\phi(n) - S$$

By the preceding proposition, $S' = S$ and so $2S = n\phi(n)$. Dividing both sides by 2 yields the claim, as desired. ■

5.3 Counting divisors

The following proposition might be a handy tool to count the number of divisors.

Proposition 5.4. Let $m \in \mathbb{Z}$ such that $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where p_i are distinct primes and $a_i \in \mathbb{N}$. Then, the number of divisors, $\#d$, of m is

$$\#d = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

Proof. Exercise. ■

We now give a remarkable fact that the sum of the totient function of **all** positive divisors of a number is in fact the number itself.

Proposition 5.5. Let $m \in \mathbb{N}$. Then

$$\sum_{0<d|m} \phi(d) = m$$

where the summation is over all positive divisors d of m.

Remark. A strong highlight on the word **all** positive divisors.

Let us get some feel of how it works via an example.

Example. Let $m = 8$. Then the positive divisors of m are $1, 2, 4$ and 8. We have

$$\phi(1) + \phi(2) + \phi(4) + \phi(8) = 1 + 1 + 2 + 4 = 8$$

Instead of directly proving the general case, we will first prove the case where m is a prime power first.

Lemma 5.6. Let p be a prime, $k \in \mathbb{N}$. Then

$$\sum_{0<d|p^k} \phi(d) = p^k$$

Proof. The positive divisors of p^k are $1, p, p^2, \ldots, p^k$. There are $k+1$ of them. Then

$$\begin{aligned}\sum_{0<d|p^k}\phi(d) &= \phi(1)+\phi(p)+\phi(p^2)+\ldots+\phi(p^k)\\ &= 1+(p-1)+p(p-1)+\ldots+p^{k-1}(p-1)\\ &= 1+p-1+p^2-p+\ldots p^k-p^{k-1}\\ &= p^k\end{aligned}$$

■

We can now prove the main proposition.

Proof. Suppose $m = p_1^{a_1}\cdots p_k^{a_k}$, where p_i are distinct prime numbers and a_i are positive integers. Now, any divisor d of m has the form $d = p_1^{x_1}\cdots p_k^{x_k}$ where $0 \leqslant x_i \leqslant a_i$ for all i. Then, we have

$$\begin{aligned}\sum_{0<d|m}\phi(d) &= \sum_{0\leqslant x_1\leqslant a_1}\cdots\sum_{0\leqslant x_k\leqslant a_k}\phi(p_1^{x_1}\cdots p_k^{x_k})\\ &= \sum_{0\leqslant x_1\leqslant a_1}\cdots\sum_{0\leqslant x_k\leqslant a_k}\phi(p_1^{x_1})\cdots\phi(p_k^{x_k})\\ &= \left(\sum_{0\leqslant x_1\leqslant a_1}\phi(p_1^{x_1})\right)\cdots\left(\sum_{0\leqslant x_k\leqslant a_k}\phi(p_k^{x_k})\right)\\ &= \left(\sum_{0<d_1|p_1^{a_1}}\phi(d_1)\right)\cdots\left(\sum_{0<d_k|p_k^{a_k}}\phi(d_k)\right)\\ &= p_1^{a_1}\cdots p_k^{a_k}\\ &= m\end{aligned}$$

where the second last inequality follows from the previous lemma. ■

The proof is not hard, just requires some time to digest. Try around with some numbers like 90 and verify that every step in the above makes sense. Here we also give another proof of the proposition. Some people would find this easier than the previous proof.

Proof. (Alternate Proof). Let S_d be the set containing all the integers less than or equal to n such that $\gcd(a,n) = d$ i.e.

$$S_d = \{a \in \mathbb{Z} : 1 \leqslant a \leqslant n \text{ and } \gcd(a,n) = d\}$$

Note that $\gcd(a,n) = d$ if and only if a/d and n/d are coprime integers. This is an equivalent statement. Thus, we have that the number of integers in S_d equals to the number of integers in $\mathcal{S}'_d$ where

$$\mathcal{S}'_d = \{b \in \mathbb{Z} : 1 \leqslant b \leqslant \frac{n}{d} \text{ and } \gcd\left(b, \frac{n}{d}\right) = 1\}$$

By definition of the Euler phi function, $\phi(n/d) = |\mathcal{S}'_d| = |S_d|$. Moreover, by definition of S_d, we have that for every $1 \leqslant a \leqslant n$, there exists a positive divisor d dividing n such that $a \in S_d$. We thus have the following two observations:

1. $\bigcup_{d|n} S_d = \{1,2,\ldots,n\} \implies \left|\bigcup_{d|n} S_d\right| = n$
2. $S_d \cap S_{\tilde{d}} = \emptyset$ for all $d \neq \tilde{d}$ i.e. they are pairwise disjoint.

Example: Let $n = 9$; then $S_3 = \{a : 1 \leqslant a \leqslant 9, \gcd(a,9) = 3\} = \{3,6\}$. The elements of S'_3 which are positive integers less than or equal to $9/3 = 3$ which are coprime to $9/3 = 3$ are $\{1,3\}$. Indeed their cardinality are equal.

Because of the pairwise disjoint property, we can use this to deduce:

$$n = \left|\bigcup_{d|n} S_d\right| = \sum_{d|n} |S_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right)$$

Now, notice that as d ranges over the divisors of n, so does n/d (but in a different order, but it does not matter), so

More explanation below.

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(n)$$

■

The final equality may be confusing to some. We will try to give an explanation here (rather than leave it as an exercise). If d is a divisor of n, then $d \times \frac{n}{d} = n$, so n/d is also a divisor of n. Thus, if $d_1, d_2, \cdots, d_k$ are all divisors of n, then so are $n/d_1, n/d_2, \ldots, n/d_k$ but in a different order. It follows that:

$$\begin{aligned}\sum_{d|n} \phi\left(\frac{n}{d}\right) &= \phi\left(\frac{n}{d_1}\right) + \phi\left(\frac{n}{d_2}\right) + \cdots + \phi\left(\frac{n}{d_k}\right) \\ &= \phi(d_1) + \phi(d_2) + \cdot + f(d_k) \\ &= \sum_{d|n} \phi(d)\end{aligned}$$

Remark. Big remark! In the explanation above, the second equality **does not** mean $\phi(n/d_i) = \phi(d_i)$ for any i!

Example. Consider $n = 10$. The divisors of n are thus $1, 2, 5, 10$. Assign a name to each divisor, $d_1 = 1, d_2 = 10, d_3 = 2, d_4 = 5$. Then, obviously n/d_i are also divisors of n for all i. We have

$$\begin{aligned}\frac{n}{d_1} &= \frac{10}{1} = 10 = d_2 \\ \frac{n}{d_2} &= \frac{10}{10} = 1 = d_1 \\ \frac{n}{d_3} &= \frac{10}{2} = 5 = d_4 \\ \frac{n}{d_4} &= \frac{10}{5} = 2 = d_3\end{aligned}$$

It follows that $\phi(n/d_1) = \phi(d_2), \phi(n/d_2) = \phi(d_1)$ etc. in this example.

So, it is clear now that n/d_i are the same divisors d_i but in a different order. In the example above we have $1 \mapsto 2$ and vice-versa and $3 \mapsto 4$ and vice-versa. A priori, we could have different mappings. It does not really matter because at the end of the day, the main result still holds.

Exercise. Give a proof of Proposition (5.5) using Group Theory. *Hint: Let $G = \langle a \rangle$ be the cyclic group of order n (generated by a). Then what does Lagrange's Theorem tells you?*

5.4 A theorem of Fermat and Euler

Theorem 5.7. (Fermat-Euler). Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$. If $\gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Proof. Let's appeal to Group Theory, just because we can. By definition $\phi(m) = |\mathbb{Z}_m^\times|$. Since $\gcd(a, m) = 1$, $[a]_m \in \mathbb{Z}_m^\times$. By Lagrange's Theorem, the order of the cyclic subgroup generated by $[a]_m$ divides the order of $\mathbb{Z}_m^\times$ i.e. it divides $\phi(m)$ so consequently $[a]_m^{\phi(m)} = [1]_m$. Equivalently, we have $a^{\phi(m)} \equiv 1 \pmod{m}$. ■

Exercise. Give a pure number-theoretic proof of this theorem.

Corollary 5.4 (Fermat's little Theorem). Let p be a prime. Then

(i) $a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}$ such that p does not divide a.

(ii) $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

Proof. There are two parts two proof.

(i). Since a is not divisible by p, we have that $\gcd(a, p) = 1$. Since p is prime, we have that $\phi(p) = p - 1$. By Fermat-Euler, we get the result.

(i). If p divides a, then the equality is trivially true as both sides are $0 \pmod{p}$. If p does not divide a, we have $\gcd(a, p) = 1$ and so by (i) we have $a^{p-1} \equiv 1 \pmod{p}$. Multiplying by a, we get the result. ■

Exercise. Give an alternate proof of this theorem. One way is to follow the same steps as when proving Fermat-Euler. Another way is to just use the induction principle on a.

Remark. Two equivalent ways of saying Fermat's little theorem are:

(1) There are p solutions in $\mathbb{Z}_p$ such that $a^p \equiv a \pmod{p}$.

(2) $a^{p-1} \equiv 0, 1 \mod p$ for all $a \in \mathbb{Z}$.

6 Primitive Roots

6.1 What are exactly primitive roots?

We will now dedicate our time to understand more about the structure of the multiplicative group of integers modulo m, $\mathbb{Z}_m^\times$. This section assumes you know some basic group theory. First, we start by recalling some definitions.

Let G be a finite group with group multiplication $\cdot$ and identity e. The order of G is defined to be the number of elements in G. If $g \in G$, then the order of g, which we will denote as $o(g)$, is defined to be the least $i \in \mathbb{N}$ such that $g^i = e$. The order $o(g)$ is also the order of the cyclic subgroup generated by g, that is the group:

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{o(g)-1}\}$$

Exercise. Good refresher, check this is a subgroup of G.

Theorem 6.1. (Lagrange's Theorem). Let G be a finite group and H a subgroup of G. Then $|H| \,|\, |G|$.

Corollary 6.1. Let G be a finite group and let $g \in G$. Then $o(g) \,|\, |G|$.

Theorem 6.2. Let $g \in G$ and $i \in \mathbb{Z}$. Then

$$g^i = e \iff o(g) \,|\, i$$

Proposition 6.1. Let $n > 1$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

(1) $o([a]_n) = o([a+n]_n)$.

(2) If $m > 1$ is a natural number such that $m \mid n$, then $o([a]_m) \mid o([a]_n)$.

(3) If $o([a]_n) = \lambda$ and $k \in \mathbb{N}$, then $o([a^k]_n) = \frac{\lambda}{\gcd(\lambda, k)}$.

(4) If $k \in \mathbb{N}$, then $o([a^k]_n) = o([a]_n) \Leftrightarrow \gcd(o([a]_n), k) = 1$.

(5) If $o([a]_n) = \lambda$, then the set $\{a, a^2, \ldots, a^\lambda\}$ has exactly $\phi(\lambda)$ elements of order λ modulo n.

Proof. For proof, see Neto's Excursion page 285. ■

Definition 6.1. A finite group G is called **cyclic** if there exists $g \in G$ such that $o(g) = |G|$. Such an element g is called a **generator** of G.

Remark. If g is a generator of a finite cyclic group G, then

$$G = \{e, g, g^2, \ldots, g^{o(g)-1}\} = \langle g \rangle$$

Here is a new definition that will be the central theme of this section.

Definition 6.2. Let $m \in \mathbb{N}$. An integer $a \in \mathbb{Z}$ is called a **primitive root** modulo m if $\gcd(a, m) = 1$ and $[a]_m$ is a generator of $\mathbb{Z}_m^\times$.

We may (although rarely) refer to this as PR (primitive root) mod m for brevity.

Remark. A more compact version of this definition is the following: An element $a \in \mathbb{Z}_m^\times$ is called a primitive root modulo m if $o(a) = \phi(m)$.

Remark. If a is a primitive root modulo m, then $\mathbb{Z}_m^\times = \{[a], [a]^2, \ldots, [a]^{\phi(m)}\}$.

Remark. A *primitive root* is a (kind of) fancy way to say that something is a generator.

Remark. If $\mathbb{Z}_m^\times$ is cyclic and $a \in \mathbb{Z}_m^\times$ is a generator, then we will refer to the congruence class a as a primitive root.

We have recalled some definitions, we have restate what does it mean for a group to be cyclic, we have even introduce a new number theoretic notion. A natural question to ask now is the following:

"For which $m \in \mathbb{N}$ is $\mathbb{Z}_m^\times$ cyclic?"

We will highlight in **red** whenever a partial answer to this question is achieved.

Prior to our definition of primitive roots, this question is equivalent to asking for which m does there exists an integer a that is coprime to m such that $o(a) = \phi(m)$. If such a exists, then $\mathbb{Z}_m^\times$ is cyclic. If such a exists, it generates $\mathbb{Z}_m^\times$. If such a exists, then a is a primitive root modulo m. We have now turn our original group theoretic problem into a number theoretic problem. Let's see an example.

Example. Let $m = 5$. Then $\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$ and $o([2]) = 4 = \phi(5) = |\mathbb{Z}_5^\times|$. So $\mathbb{Z}_5^\times$ is cyclic with $[2]$ as a generator.

Example. Let $m = 8$, $\mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$. It is easy to calculate that $o([1]) = 1$, $o([3]) = o([5]) = o([7]) = 2$. So no element has order 4 and hence $\mathbb{Z}_8^\times$ is not cyclic.

One natural way to dive into this problem is by finding a certain criteria to detect whether something is a primitive root or not.

Lemma 6.3. (Primitive Root Test). Let $m \in \mathbb{N}$ and $\gcd(a, m) = 1$. Then, $a \in \mathbb{Z}$ is a primitive root modulo m if and only if

$$a^{\phi(m)/p} \not\equiv 1 \pmod{m}$$

for all prime divisors p of $\phi(m)$.

Proof. Exercise. ∎

It turns out, if you have one primitive root, then you have all of them.

Theorem 6.4. Let $m \in \mathbb{N}$ and suppose a is a primitive root modulo m. Then

$$a^k \text{ is a primitive root modulo } m \iff \gcd(k, \phi(m)) = 1.$$

Proof. We resort to basic Group Theory. If a has order $\phi(m)$, then a^k has order $\phi(m)/\gcd(\phi(m), k)$. So, a^k has order $\phi(m)$ exactly when $\gcd(\phi(m), k) = 1$. ∎

Proof. Alternate proof. We use pure number theory. Let $d = \gcd(k, \phi(m)$. Then

$$\begin{aligned}(a^k)^n \equiv 1 \pmod m &\iff a^{kn} \equiv 1 \pmod m \\ &\iff \phi(m) \text{ divides } kn \\ &\iff \frac{\phi(m)}{d} d \text{ divides } \frac{k}{d} dn \\ &\iff \frac{\phi(m)}{d} \text{ divides } \frac{k}{d} n \\ &\iff \frac{\phi(m)}{d} \text{ divides } n\end{aligned}$$

where the final iff is because $\gcd\left(\frac{\phi(m)}{d}, \frac{k}{d}\right) = \frac{1}{d}\gcd(\phi(m), k) = 1$. ∎

6.2 Existence of Primitive Roots

This subsection is dedicated to understanding when do primitive roots exists.

6.2.1 Trivial case

The trivial cases are those of which we can check by hand. We have these for free.

Proposition 6.2. $\mathbb{Z}_1^\times, \mathbb{Z}_2^\times$ and $\mathbb{Z}_4^\times$ are cyclic.

Proof. We do this by direct inspection. $\mathbb{Z}_1^\times = \{[1]\}$, so clearly $[1]$ generates $\mathbb{Z}_1^\times$. $\mathbb{Z}_2^\times = \{[1], [2]\}$ and obviously $[2]$ generates $\mathbb{Z}_2^\times$. Finally, $\mathbb{Z}_4\times = \{[1], [3]\}$ and $[3]$ generates $\mathbb{Z}_4^\times$. ∎

Let us check multiplicative groups modulo p for small primes. $\mathbb{Z}_3^\times = \{[1], [2]\}$ and $[2]$ generates this group. $\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$ and $[2]$ generates this group. One can check that $[3]$ generates $\mathbb{Z}_7^\times$, $[2]$ generates $\mathbb{Z}_{11}^\times$, $[2]$ also generates $\mathbb{Z}_{13}^\times$, $[3]$ generates $\mathbb{Z}_{17}^\times$ and $[5]$ generates $\mathbb{Z}_{23}^\times$. Here, we start to see a pattern and conjecture that the multiplicative groups modulo p where p is prime is cyclic. This turns out to be true!

6.2.2 Prime case

Theorem 6.5. Let p be a prime number. Then, $\mathbb{Z}_p^\times$ is cyclic.

The idea of the proof is the following. Consider the ℓ.c.m of all the elements in $\mathbb{Z}_p^\times$ and for contradiction, we will assume this is less than $\phi(p)$. The ℓ.c.m is divisible by all other lower orders. So any element in $\mathbb{Z}_p^\times$ to the power of this order is 1 modulo p and there are $\phi(p)$ of them . This contradicts Lagrange's Theorem for polynomials.

Proof. Suppose $\mathbb{Z}_p^\times$ is not cyclic. Define ℓ to be **the lowest common multiple of the order of all elements** $[a] \in \mathbb{Z}_p^\times$. By hypothesis[12], $\ell < \phi(p) = p - 1$. But then, we have that

$$a^\ell \equiv a^{o(a)k} \equiv (a^{o(a)})^k \equiv 1 \pmod p$$

for all $[a] \in \mathbb{Z}_p^\times$ where k is an arbitrary integer. Since, we have $p - 1$ elements in $\mathbb{Z}_p^\times$, this implies that there are $p - 1$ solutions to the congruence equation $X^\ell - 1 \equiv 0 \pmod p$. Since p is prime, this violates Lagrange's Theorem on polynomials (Theorem 4.9) because we assumed $\ell < p - 1$. ∎

[12] *If $\mathbb{Z}_p^\times$ is cyclic, then there is an element of order $p - 1$, so then $\ell = p - 1$.*

Remark. The converse is false! Consider $\mathbb{Z}_6^\times = \{[1], [5]\}$. So, $\phi(6) = 2$. We have $5^2 \equiv 25 \equiv 1 \pmod 6$, so $o(5) = 2$ and hence $\mathbb{Z}_6^\times$ is cyclic. But, 6 is definitely not prime.

We could have also proven this theorem by proving[13] the existence of a primitive root for every prime p. This idea would also use Lagrange's theorem for polynomials mod p. Great, we have that $\mathbb{Z}_p^\times$ **is cyclic**.

[13] *refer Rosen page. 357*

6.2.3 The not easy p^k case

Our goal now is to hunt the primitive roots modulo prime powers modulus i.e. the case $m = p^k$ for some $k \in \mathbb{N}$. Unfortunately as we will see, this wouldn't hold for all primes.

Let's deal with the case $k = 2$ first. We will show that if an integer is a primitive root modulo p (which exists, we proved this!), then this integer could, in some way, be a primitive root modulo p^2.

Proposition 6.3. Let p be a prime number. Suppose a is a primitive root modulo p. Then, either a or $a + p$ (or both) is a primitive root modulo p^2.

The goal is to find an element of $\mathbb{Z}_{p^2}^\times$ with order $\phi(p^2) = p(p-1)$. Our best candidate is a and $a + p$ (we will see why in the proof).

Proof. Let's look at the data given.

Unravelling the Data. Since a is a primitive root modulo p, then $o([a]_p) = \phi(p) = p - 1$. Moreover, we know[14] that $o([a+p]_p) = o([a]_p) = p - 1$.

[14] $[a]_p = [a+p]_p$, *so they must have the same order.*

We know order of an element in a finite group divides the order of the group by Lagrange's Theorem. In particular, we know

$$o([a]_{p^2}) \mid \phi(p^2) = p(p-1) \qquad (*)$$

and similarly, $o([a+p]_{p^2})$ divides $p(p-1)$.

Furthermore, we know that since $a^{o([a]_{p^2})} \equiv 1 \pmod{p^2}$, then $a^{o([a]_{p^2})} \equiv 1 \pmod p$. So, we have

$$p - 1 = o([a]_p) \mid o([a]_{p^2}) \qquad (\dagger)$$

The equality is true because a is a primitive root modulo p. Similarly, $p - 1$ divides $o([a+p]_{p^2})$.

The actual proof. We claim that either a or $a + p$ is a primitive root modulo p^2. Combining $(*)$ and $(\dagger)$, we have that

$$p - 1 \mid o([a]_{p^2}) \mid p(p-1)$$

and

$$p - 1 \mid o([a+p]_{p^2}) \mid p(p-1)$$

Hmm, what number is divisible by $p - 1$ and divides $p(p-1)$? Well, considering the prime factorization of such number, we must have that this number must be either $p - 1$ or $p(p-1)$.

Example: Take $p = 3$, then $p - 1 = 2$ and $p(p-1) = 6$. Suppose ω is a number that is divisble by 2 and 6. What could ω possibly be? Well it must be between 2 and 6 for sure, so it must be in $\{2, 3, 4, 5, 6\}$. It is now trivial to see that it must be either 2 or 6.

If $o([a]_{p^2}) = p(p-1)$, we are done. 😄

So, suppose $o([a]_{p^2}) = p-1$. Recall that $o([a+p]_{p^2})$ can also be either $p-1$ or $p(p-1)$. Our goal now is to show that $o([a+p]_{p^2})$ cannot be $p-1$. Well the obvious way is to compute:

$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)pa^{p-2} \equiv a^{p-1} + p^2a^{p-2} - pa^{p-2} \pmod{p^2}$$

Since we assumed $o([a]_{p^2}) = p-1$, a^{p-1} is 1 modulo p^2. We also have $p^2a^{p-2} \equiv 0 \pmod{p^2}$ for obvious reasons. We are left with

$$(a+p)^{p-1} \equiv 1 - pa^{p-2} \pmod{p^2} \tag{6.1}$$

Since $\gcd(a,p) = 1$, we must have that $\gcd(a,p^2) = 1$ by Lemma (5.1) i.e. a and p^2 are coprime that is a^{p-2} is not 0 modulo p^2. So, (6.1) is not 1 modulo p^2 implying that $o([a+p]_{p^2})$ cannot be $p-1$ 😄. Thus, $o([a+p]_{p^2})$ must have order $p(p-1)$. ■

Remark. Important remark! Order of an element depends on the group! In general, $o([a]_p) \neq o([a]_{p^2})$. We're in different groups here $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$. An easy example would be 2 (mod 3) has order 2 while 2 (mod 3^2) has order 6 (note that $\phi(3^2) = 6$).

Remark. The other way around is *obvious*. If a is a primitive root modulo p^2, then it is automatically a primitive root modulo p.

To see this, if a is a primitive root modulo p^2, then $\mathbb{Z}_{p^2}^\times = \{[a], [a]^2, \ldots, [a]^{p^2}\}$. This means that there is a positive integer k such that $a^k \equiv b \pmod{p^2}$ for every $[b] \in \mathbb{Z}_{p^2}^\times$. But, if p^2 divides $a^k - b$, then p divides $a^k - b$. So, a also generates $\mathbb{Z}_p^\times$.

Exercise. Convince yourself that the remark above is true for $p = 7^3 = 343$. Use Mathematica with the function PrimitiveRootList[343]. Then reduce mod 7^2 and 7 by applying the function Mod[·, 49] and Mod[·, 7] respectively.

Proposition (6.3) is a gift. First, it implies that $\mathbb{Z}_{p^2}^\times$ **is cyclic**. That is, it tells us the existence of primitive roots modulo p^2. Secondly, **it gives a procedure on how to find a primitive root mod p^2 if we already know a primitive root mod p.**

Looking at the proof of Proposition (6.3) carefully, we can actually restate it into a more precise statement.

Proposition 6.4. Let p be a prime number, and suppose a is a primitive root mod p. Then

$$a \text{ is a primitive root mod } p^2 \iff a^{p-1} \not\equiv 1 \pmod{p^2}.$$

Proof. The proof is basically the proof as the proposition above. We have $o([a]_{p^2}) | \phi(p^2) = p(p-1)$, this is a fact. Moreover,

$$a^{o([a]_{p^2})} \equiv 1 \pmod{p^2} \implies a^{o([a]_{p^2})} \equiv 1 \pmod{p}$$

by divisibility. But a is primitive mod p, so $p-1 = \phi(p) \mid o([a]_{p^2})$. Accordingly, $o([a]_{p^2})$ is either $p-1$ or $p(p-1)$. But $o([a]_{p^2}) = p-1$ implies that

$$a^{p-1} \equiv 1 \pmod{p^2}$$

which we assumed cannot be. So $o([a]_{p^2}) = p(p-1) = \phi(p^2)$ and so a is primitive mod p^2.

The proof of the converse to this theorem is a bit lengthy, so we will omit it. For proof, cf. Apostol. ■

Corollary 6.2. If a is a primitive root modulo p, then $a^p + p$ is a primitive root modulo p^2.

Proof. By Fermat's little theorem, $a^p \equiv a \pmod{p}$. Because a is a primitive root modulo p, anything congruent to a is a primitive root modulo p, thus a^p is a primitive root modulo p. However,

$$a^{p(p-1)} \equiv 1 \pmod{p^2}$$

so $o([a^p]_{p^2}) < \phi(p^2)$. Thus, a^p is not a primitive root modulo p^2. By Proposition (6.3), $a^p + p$ is a primitive root modulo p^2. ■

Lemma 6.6. Let p be a prime number, and suppose a is a primitive root modulo p. Then there are exactly p elements of $\mathbb{Z}_{p^2}^\times$ that are congruent to a modulo p.

Proof. Still in search of a proof, looks legit. ■

Theorem 6.7. Let p be a prime number, and suppose a is a primitive root modulo p. Then there are exactly $\phi(p)$ primitive roots modulo p^2 that are congruent to a modulo p.

Proof. By Hensel's Lemma, there is exactly one $[x]$ of $\mathbb{Z}_{p^2}^\times$ congruent to a modulo p satisfying $x^{p-1} \equiv 1 \pmod{p^2}$. Moreover, we now know by the preceding proposition that a is a primitive root modulo p^2 if and only if $a^{p-1} \not\equiv 1 \pmod{p^2}$. Accordingly, out of the p elements of $\mathbb{Z}_{p^2}^\times$ congruent to a modulo p (we know this from the preceding lemma), only one of them has order $p-1$ and the other $p-1$ elements has order $p(p-1) = \phi(p^2)$. Therefore, there are exactly $p - 1 = \phi(p)$ primitive roots modulo p^2 that are congruent to a modulo p, as desired. ■

It turns out that we could do better! We will now show that if we have a primitive root mod p^2 (which we now know always exists), then it is also a primitive root modulo p^k for all $k \geqslant 2$. But, here is a warning. It doesn't always work. We need p to be an odd prime!

Proposition 6.5. Let p be an odd prime. Suppose a is a primitive root modulo p^2. Then, a is a primitive root modulo p^k for all $k \geqslant 2$.

Remark. p has to be an **ODD** prime. ODD prime. ODD prime.

> **Example.** Let $p = 2$. Then $\mathbb{Z}_{2^3}^\times = \mathbb{Z}_8^\times$ is NOT cyclic. Every element has order 1 or 2 but $\phi(8) = 4$.

The only case when a power of even prime ($p = 2$) is cyclic is $\mathbb{Z}_4^\times$.

Remark. We assume a is a primitive root modulo p^2 here. **modulo *p*-squared**. Being a primitive root modulo p is not enough as we have seen in Proposition (6.3) that there could be two cases - either the number itself **or** the number plus p is a primitive root modulo p^2.

Before we start with the proof, we just want to remind you to **pay attention to the powers of the prime**.

Proof. We prove by induction on k.

Base Case. The case $k = 2$ is true by assumption.

Inductive Step. Suppose the conclusion is true up to some k i.e. $a \in \mathbb{Z}$ is a primitive rood modulo p^k for finitely many $k \geqslant 2$.

$(k+1)$-th case . We need to show a is a primitive rood modulo p^{k+1}. Let us see what data we have and what we can do to them.

Unravelling the Data. As in the previous proof, we know that:

$$\phi(p^k) = o([a]_{p^k}) \mid o([a]_{p^{k+1}}) \mid \phi(p^{k+1}) \qquad (*)$$

The **green** equality is true by the induction hypothesis. We have

$$\phi(p^k) = p^{k-1}(p-1)$$
$$\phi(p^{k+1}) = p^k(p-1)$$

Since $k \geqslant 2$, we can do this:

$$a^{p^{k-1}(p-1)} = \left(a^{p^{k-2}(p-1)}\right)^p \qquad (**)$$

But note that

$$a^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \qquad (\#)$$

since order of a modulo p^k is $\phi(p^k) = p^{k-1}(p-1) \neq p^{k-2}(p-1)$.

Since a is a primitive root modulo p^k up to some k by the induction hypothesis, we know it is a primitive root modulo p^{k-1}. In particular, it is coprime to p^{k-1}. So, by Fermat-Euler

$$a^{\phi(p^{k-1})} \equiv a^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}} \qquad (\dagger)$$

$(\#)$ combining with $(\dagger)$ implies that there exists an integer λ such that $a^{p^{k-2}(p-1)} = 1 + p^{k-1}\lambda$ such that p does not divide λ. We will denote this fact as $(\dagger\dagger)$.

the orange colour highlighted here means that they are related to one another.

Actual proof. From $(*)$, since $o([a]_{p^{k+1}})$ is sandwiched by these two numbers, then we have $o([a]_{p^{k+1}})$ to be $p^{k-1}(p-1)$ or $p^k(p-1)$.

If $o([a]_{p^{k+1}}) = p^k(p-1)$, we are done. 😊

So, suppose $o([a]_{p^{k+1}}) = p^{k-1}(p-1)$. Our goal is to show that this is rubbish. An obvious way is to just raise a to the $p^{k-1}(p-1)$ power and hope that it is not 1 modulo p^{k+1}, otherwise this is not rubbish. Now, we have

$$a^{p^{k-1}(p-1)} \overset{(**)}{=} \left(a^{p^{k-2}(p-1)}\right)^p \overset{(\dagger\dagger)}{=} (1 + p^{k-1}\lambda)^p \overset{\text{(Binomial expansion}^{15})}{\equiv} 1 + p^k\lambda + \binom{p}{2} p^{2k-2}\lambda^2 \pmod{p^{k+1}}$$

[15] *since $i \geqslant 2$, p^{k+1} divides $(p^{k-1}\lambda)^3, (p^{k-1}\lambda)^4, \cdots$, so they all die modulo p^{k+1}. In-depth explanation below.*

Since p **is an odd prime**, we have that $p \mid \binom{p}{2}$. This implies $p^{k+1} \mid \binom{p}{2} p^{2k-2}$. It follows that

If p even i.e. $p = 2$, then $\binom{p}{2} = \binom{2}{2} = 1$ which is not divisible by $p = 2$.

$$a^{p^{k-1}(p-1)} \equiv 1 + p^k\lambda \pmod{p^{k+1}}$$

Since p does not divide λ, it follows that $p^k\lambda \not\equiv 0 \pmod{p^{k+1}}$. The claim follows. 😊 ■

Remark. We really do need p to be odd here! Otherwise the proof won't work.

Remark. We will show in detail the binomial expansion step. This is actually is similar to when we did for the proof of the lemma before Hensel's Lemma. Unfortunately, we can't use that result here (why?). Now

$$(1+p^{k-1}\lambda)^p = \sum_{i=0}^{p} \binom{p}{i} (1)^{p-i}(p^{k-1}\lambda)^i$$

Now p^{k+1} divides $p^{(k-1)i}$ (and hence, $(p^{(k-1)}\lambda)^i$) iff $k+1 \leqslant (k-1)i$ which is true iff $k(i-1) \geqslant i+1$. By assumption, $k \geqslant 2$. So, this is true iff $i-1 \geqslant 3/2$. Since i is an integer, this is equivalent to $i \geqslant 3$. So, for all $i \geqslant 3$, $p^{(k-1)i}$ dies. This leave us with the first three terms of the expansion as seen in the proof.

The consequence of this proposition is that **if p is an odd prime, then $\mathbb{Z}_{p^k}^\times$ is cyclic for all $k \geqslant 1$.**

Corollary 6.3. 2 is a primitive root modulo 3^k and modulo 5^k, for every $k \in \mathbb{N}$.

Proof. The case $k = 1$ is clear by brute-forcing. Suppose $k \geqslant 2$. It suffices to show that 2 is a primitive rood modulo 9 and 25 (respectively) as then, by the preceding theorem we will get our desired result. Since $\phi(9) = 6$, we have $o([a]_9) \mid 6$. However, since none of $2^1, 2^2$ or 2^3 is a multiple of 9, we must have that $o([a]_9) = 6 = \phi(9)$. Thus 2 is a PR mod 9. It is completely analogous to show that 2 is a PR mod 25. ■

Proposition 6.6. Let p be a prime number and $n \in \mathbb{N}$. Then

$$1^n + 2^n + \ldots + (p-1)^n = \begin{cases} 0 \pmod p & \text{if } (p-1) \nmid n \\ -1 \pmod p & \text{if } (p-1) \mid n \end{cases}$$

Proof. For proof, cf. page 292 Neto's Excursion. ■

6.2.4 The $2p^k$ case

Remarkably, we discovered that for every **odd prime** power, there exists a primitive root. Can we push this a little bit and ask what about twice an odd prime power, would there still exist a primitive root? How about thrice an odd prime power or maybe four times an odd prime power?

Well, we could find counter-examples for the case thrice and four times an odd prime power without much hassle.

Example. Consider $p = 5^2$. Then thrice this is 75. $\mathbb{Z}_{75}^\times$ is not cyclic. Four times of p is 100. $\mathbb{Z}_{100}^\times$ is also not cyclic. Check this using Mathematica or Python.

Theorem 6.8. Let p be an odd prime and $k \geqslant 2$. Then, $\mathbb{Z}_{2p^k}^\times$ is cyclic.

Proof. By the Chinese Remainder Theorem restricted to units (5.2), there is an isomorphism (of groups)

$$\mathbb{Z}_{2p^k}^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}_{p^k}^\times$$

But $\mathbb{Z}_2^\times$ is the trivial group. Thus

$$\mathbb{Z}_{2p^k}^{\times} \cong \mathbb{Z}_{p^k}^{\times}$$

We have proven that $\mathbb{Z}_{p^k}^{\times}$ is cyclic, so $\mathbb{Z}_{2p^k}^{\times}$ must be cyclic. Moreover, if a generates $\mathbb{Z}_{p^k}^{\times}$, then either a or $a + p^k$ (the one that is odd) generates $\mathbb{Z}_{2p^k}^{\times}$. ■

This theorem is equivalent to saying that if a is a primitive root modulo p^k, then either a or $a + p^k$ (the one that is odd) is a primitive root modulo $2p^k$. It sounds similar to Theorem (6.3). In fact, we can prove this theorem in a very similar way to proving that theorem since we now know a primitive root modulo p^k exists for all $k \geqslant 1$. So, we have that $\mathbb{Z}_{2p^k}^{\times}$ **is cyclic for all** $k \geqslant 1$.

Exercise. Prove that $\mathbb{Z}_{2p^k}^{\times}$ is cyclic using the method as in proving Theorem (6.3).

6.2.5 Gauss's complete criterion

We will now give the answer to our main question earlier,

"For which $m \in \mathbb{N}$ is $\mathbb{Z}_m^{\times}$ cyclic?"

This is the most important result of this section. It was firstly proven by Gauß (Gauss) in his great *Disquisitiones Arithmeticae* (1801). This theorem is sometimes called the Primitive Root Theorem. We will just refer to it as Gauss's Theorem on Primitive Roots.

Theorem 6.9. (Gauss). Let $m \in \mathbb{N}$. Then, $\mathbb{Z}_m^{\times}$ is cyclic if and only if $m = 1, 2, 4, p^k$ or $2p^k$ for some **odd** prime p and $k \in \mathbb{N}$.

We can restate the statement as: Let $m \in \mathbb{N}$. Then, there exists a primitive root modulo m if and only if $m = 1, 2, 4, p^k$ or $2p^k$ for some odd prime p and $k \in \mathbb{N}$.

Note that we have proven the ($\Longleftarrow$) direction of the proof (cf. Prop. (6.2), Theorem (6.5), Prop. (6.3), Prop. (6.5) and Theorem (6.8)). What's left of Gauss's Theorem is the ($\Longrightarrow$) direction. We will give a proof now.

Proof. ($\Longrightarrow$). We proof by contradiction. Suppose that m is not $1, 2, 4, p^k$ or $2p^k$ for some odd prime p where $k \in \mathbb{N}$. Then, m can only admit two forms. Either $m = 2^j$ for some $j \geqslant 3$ or $m = ab$ where $a, b \geqslant 3$ and $\gcd(a, b) = 1$.

Case I. Suppose $m = 2^j$ for some $j \geqslant 3$. Then, there exists a surjective (group) homomorphism

$$\mathbb{Z}_m^{\times} \to \mathbb{Z}_{2^3}^{\times}$$

Since surjective homomorphisms preserves cyclicity. $\mathbb{Z}_8^{\times}$ being not cyclic, implies $\mathbb{Z}_m^{\times}$ cannot be cyclic [↯].

Case II. Suppose $m = ab$ where $a, b \geqslant 3$ and $\gcd(a, b) = 1$. Then $\phi(m) = \phi(a)\phi(b)$. Since $a, b \geqslant 3$, by Prop. (5.2), we have that $\phi(a), \phi(b)$ both being even. Thus, 2 divides $\gcd(\phi(a), \phi(b))$. In particular, $\gcd(\phi(a), \phi(b)) > 1$. This implies $\ell := \operatorname{lcm}(\phi(a), \phi(b)) < \phi(a)\phi(b) = \phi(m)$.

Now suppose $\lambda \in \mathbb{Z}$ is coprime to m. Then, λ has to be coprime to a and b. Furthermore, by Fermat-Euler, we have that $\lambda^{\phi(a)} \equiv 1 \pmod{a}$ and $\lambda^{\phi(b)} \equiv 1 \pmod{b}$. This implies that $\lambda^{\ell} \equiv 1 \pmod{a}$ and $\lambda^{\ell} \equiv 1 \pmod{b}$. Since a and b are coprime, we have

$$\lambda^{\ell} \equiv 1 \pmod{m}$$

recall that if x, y are non-zero integers (otherwise lcm wouldn't even be defined!), then $\operatorname{lcm}(x, y)\gcd(x, y) = |xy|$. If $\gcd(x, y) = 1$, then $\operatorname{lcm}(x, y) = |xy|$. If $\gcd(x, y) > 1$, then $\operatorname{lcm}(x, y) = |xy|/\gcd(x, y) < |xy|$.

But $\ell < \phi(m)$. So this implies that every element of $\mathbb{Z}_m^\times$ has order less than $\phi(m)$. Thus, $\mathbb{Z}_m^\times$ cannot be cyclic [↯]. ■

recall that the order of g is the smallest positive integer i such that $g^i = 1$. $\lambda^\ell \equiv 1 \pmod m$ implies that $o(\lambda) \mid \ell$. Since, ℓ is non-zero, we have $o(\lambda) \leqslant \ell < \phi(m)$. Particularly, $o(\lambda) < \phi(m)$, so there are no $\lambda \in \mathbb{Z}_m^\times$ that generates the group.

Theorem 6.10. Let $m \in \mathbb{N}$. If $\mathbb{Z}_m^\times$ has a primitive root, then the number of primitive roots in $\mathbb{Z}_m^\times$ is $\phi(\phi(m))$.

We will borrow this theorem from Group Theory: Let G be a group, $g \in G$ has order d (in particular it is not infinite) and $a \in \mathbb{Z}$. Then g^a has order $d/\gcd(a,d)$.

Proof. Suppose g is a primitive root modulo m i.e. $\mathbb{Z}_m^\times = \{[g], [g]^2, \ldots, [g]^{\phi(m)}\}$. Then, g must have order $\phi(m)$. Furthermore, g^k has order $\phi(m)/\gcd(k, \phi(m))$. The only way for g^k to be a primitive root is if $\gcd(k, \phi(m)) = 1$ i.e. k and $\phi(m)$ are coprime. So, we are now counting the number of integers in the set

$$\{a \in \mathbb{Z} : 1 \leqslant a \leqslant \phi(m) \text{ and } \gcd(a, \phi(m)) = 1)\}$$

There are $\phi(\phi(m))$ of them. ■

Below seems like trivial results in comparison to the other results proven in this section but they are exceptionally useful in computations.

Proposition 6.7. Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ be a primitive root modulo m.

(1). If $b \in \mathbb{Z}$ is coprime to m, then there exists $i \in \mathbb{N} \cup \{0\}$ such that $b \equiv a^i \pmod m$. In fact, this i is unique with $1 \leqslant i \leqslant \phi(m)$.

(2). Let $i, j \in \mathbb{N} \cup \{0\}$. Then,

$$a^i \equiv a^j \pmod m \iff i \equiv j \pmod{\phi(m)}$$

Proof. Two parts to the proof.

(1). Since $a \in \mathbb{Z}$ is a primitive root modulo m, $[a]$ generates $\mathbb{Z}_m^\times$ i.e. $\mathbb{Z}_m^\times = \{[a], [a]^2, \ldots, [a]^{\phi(m)}\}$. Since b is coprime to m, $[b] \in \mathbb{Z}_m^\times$. In particular, $[b] = [a]^i$ for a unique i where $1 \leqslant i \leqslant \phi(m)$. Being equal as congruence classes modulo m is the same as being equivalent modulo m.

(2). Suppose $a^i \equiv a^j \pmod m$. Then, because $\gcd(a, m) = 1$, there is an inverse. We have $a^{i-j} \equiv 1 \pmod m$. This is true if and only if $o(a)$ divides $(i - j)$. Since $\phi(m) = o(a)$, we have $\phi(m)$ dividing $(i - j)$. This is equivalent to $i \equiv j \pmod{\phi(m)}$.

Note that each step in part (2) of the proof is an *if and only if* statement, so we really have proven the claim in both directions. ■

6.2.6 Departure.

Before departing from this section, we will give a summary to what we have done.

Summary. This section is summarized as below.

(1). **What is it?** a is a primitive root modulo m if $o([a]_m) = \phi(m)$ i.e.

$$\mathbb{Z}_m^\times = \{[a], [a]^2, \ldots, [a]^\phi(m)\}$$

(2). **How I.** a is a primitive root modulo m if and only if

$$a^{\phi(m)/p} \not\equiv 1 \pmod{m}$$

for all prime divisors p of $\phi(m)$.

(2). **How II.** If a is a primitive root modulo p, then a is also a primitive root modulo p^k for all $k \geqslant 1$ except the case where $a^{p-1} \equiv 1 \pmod{p^2}$. In this case $a+p$ is primitive.

(3). **How III.** If a is a primitive root modulo p^k, then it is trivially a primitive root modulo p.

(4). **How IV.** If a is a primitive root modulo p^k, then either a or $a+p^k$ (the one that is odd) is a primitive root modulo $2p^k$.

(5). **How many?** The numbers of primitive root modulo m (if it exists) is $\phi(\phi(m))$.

(6). **When?** There exists a primitive root modulo m if and only if $m = 1, 2, 4, p^k$ or $2p^k$ for some odd prime p and $k \in \mathbb{N}$.

6.3 Carmichael numbers

Definition 6.3. (Carmichael number). A composite integer n that satisfies $a^n \equiv a$ for all $a \in \mathbb{Z}$ is called a **Carmichael number**.

by compositeness, n is neither 1 nor a prime.

It is probably good to bear in mind that $561 = 3 \times 11 \times 17$ is the smallest Carmichael number.

Proposition 6.8. Every Carmichael number is odd.

Proof. Suppose n is a Carmichael number such that it is even. By definition $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. By letting $a = n-1$, we observe that

$$(-1)^n \equiv (n-1)^n \equiv n-1 \equiv -1 \pmod{n} \text{ [↯]}$$

This is a contradiction as $(-1)^n \equiv 1 \pmod{n}$ if n is even. ■

yes, this may also conclude that $n = 2$ as $(-1)^2 \equiv 1 \equiv -1 \pmod{2}$. However, a Carmichael number is by definition not a prime, so it cannot be 2.

Definition 6.4 (Squarefree). A positive integer is said to be **squarefree** if its prime factorisation contains no repeated factors.

Remark. Three things to note:

(1) All primes are trivially squarefree.

(2) The number 1 is taken to be squarefree by convention.

(3) Equivalently, we say a number is squarefree iff it is a product of distinct primes (with at most power of 1).

(4) i.e. n is squarefree if it looks like $n = p_1 p_2 \cdots p_k$ for distinct primes p_i.

note, no powers!

Proposition 6.9. Every Carmichael number is squarefree.

For a proof not using primitive roots, cf. Silverman page 134.

Proof. Suppose that n is a Carmichael number and let p be an odd[16] prime number dividing n. For the sake of contradiction, assume p divides n exactly k times. We want to show that $k = 1$.

[16] *we may assume that $p \neq 2$ as we have proven that Carmichael numbers are odd.*

Let g be a primitive root modulo p^k. This exists since p is odd. Since n is a Carmichael number, we have

$$g^n \equiv g \pmod{n} \implies g^n \equiv g \pmod{p^k}$$

the implication is true because $p^k \mid n$. Then use the fact if $d \mid m$, then $a \equiv b \pmod{m} \implies a \equiv b \pmod{d}$.

Since g is a primitive root modulo p^k, $\gcd(g, p^k) = 1$ and thus

$$g^{n-1} \equiv 1 \pmod{p^k}.$$

Accordingly, the order of g divides $n-1$. By primitivity of g, this implies $\phi(p^k) = p^{k-1}(p-1)$ divides $n-1$. By transitivity, we thus have $p^{k-1} \mid n-1$.

as $p^{k-1} \mid \phi(p^k) = p^{k-1}(p-1) \mid n-1$.

On the other hand, we assumed $p^k \mid n$. So since $p^{k-1} \mid p^k$, by transitivity we have $p^{k-1} \mid n$.

Therefore, p^{k-1} divides both $n-1$ and n. This forces us to have $p^{k-1} = 1$ and hence, $k = 1$, as desired. Since p was arbitrary, we get our desired result. ∎

A theorem that allows us to find Carmichael numbers is the following.

Theorem 6.11 (Korselt's Criterion). Let n be a composite number. Then n is a Carmichael number if and only if it is **odd** and **every** prime p dividing n satisfies the following two conditions:

(1) p^2 does not divide n

(2) $p - 1$ divides $n - 1$.

i.e. n is squarefree. Condition (1) guarantees that n is a product of distinct primes.

Proof. ($\Longleftarrow$). Suppose that n is a composite number, and suppose that every prime divisor of n satisfies condition (1) and (2). We want to show that n is a Carmichael number. Let $n = p_1 p_2 \dots p_r$. By condition (1), all the p_i are distinct. By condition (2), each $p_i - 1$ divides $n - 1$ so for each i we can factor

$$n - 1 = (p_i - 1)k_i$$

for some $k_i \in \mathbb{Z}$. Now fix any integer $a \in \mathbb{Z}$. Compute the value of $a^n \pmod{p_i}$ as follows:

1. If $p_i \mid a$, then obviously $a^n \equiv 0 \equiv a \pmod{p_i}$.
2. If p_i does not divide a. Then we can use Fermat's little Theorem to compute:

$$a^n = a^{(p_i-1)k_i+1} = (a^{p_i-1})^{k_i} \cdot a \equiv 1^{k_i} \cdot a \equiv a \pmod{p_i}.$$

We have thus proved that $a^n \equiv a \pmod{p_i}$ for all $a \in \mathbb{Z}$, for all $i = 1, 2, \dots, r$. Since $p_1, p_2, \dots, p_r$ are all distinct, we thus have, by the Chinese Remainder Theorem, that $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. By definition, n is thus a Carmichael number.

($\Longrightarrow$). We have proved that Carmichael numbers are squarefree. It remains to prove that the primes dividing n satisfies (2). In fact, we will see that the prove of this is exactly the same as proving squarefree.

Suppose n is a Carmichael number and let $p_1, p_2, \ldots, p_r$ be the primes dividing n. Then $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. For each $1 \leqslant i \leqslant r$, let g_i be a primitive root modulo p_i. Then letting $a = g$ we have

$$g_i^n \equiv g_i \pmod{n} \implies g_i^n \equiv g_i \pmod{p_i}.$$

By definition of primitive root, $\gcd(g_i, p_i) = 1$ and so there is an inverse. The congruence equation thus becomes $g_i^{n-1} \equiv 1 \pmod{p_i}$. Since g_i has order $\phi(p_i) = p_i - 1$ (by primitivity), we thus have $p_i - 1$ divides $n - 1$. Since i was arbitrary, we get our desired result. ■

Remark. Thus, we now know that Carmichael numbers look like $n = p_1 p_2 \ldots p_r$ where p_i are all odd distinct primes. Moreover every p_i satisfies $(p_i - 1) \mid (n - 1)$.

Example (due to Chernick.)**.** Suppose k is a positive integer such that $6k+1$, $12k+1$ and $18k+1$ are all prime. Then the product

$$n = (6k+1)(12k+1)(18k+1)$$

is a Carmichael number. For example, taking $k = 1$, 1729 is a Carmichael number.

Proof. Clearly n is squarefree. It remains to check (2) of Korselt's Criterion i.e. we just have to check $6k, 12k$ and $18k$ all divide $n - 1$. Since $6 \mid 12$, it suffices to check for $n \pmod{12k}$ and $n \pmod{18k}$. Modulo $12k$, we have

$$n \equiv (6k+1)(6k+1) \equiv 12k(3k) + 12k + 1 \equiv 1 \pmod{12k}.$$

here $(12k+1) \equiv 1 \pmod{12k}$ and $18k \equiv 6k \pmod{12k}$.

Modulo $18k$, we have

$$n \equiv (6k+1)(12k+1) \equiv 72k^2 + 18k + 1 \equiv 18k(4k) + 18k + 1 \equiv 1 \pmod{18k}.$$

Indeed, $n - 1$ is divisible by $6k, 12k$ and $18k$ and so by Korselt's Criterion, n is Carmichael as desired. ■

Corollary 6.4. A composite integer $n \geqslant 2$ is a Carmichael number if and only if $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ whenever $\gcd(a, n) = 1$.

to be fair here, we could have made $n \in \mathbb{N}$ (instead of $n \geqslant 2$) as $2, 3$ are not composite integers. To be pedantic, one would have written $n \geqslant 4$.

Proof. ($\implies$). If n is Carmichael, then by definition $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. If $\gcd(a, n) = 1$, there is an inverse to a mod n, so we can multiply by this on both sides to attain our desired result.

($\impliedby$). Suppose $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ whenever $\gcd(a, n) = 1$. We want to show n is a Carmichael number. We will do this by showing that n satisfies Korselt's criterion. If n is even, then $n - 1$ is odd. Accordingly, $(-1)^{n-1} \equiv -1 \not\equiv 1 \pmod{n}$ [7]. So n has to be odd.

Let p be an odd prime number dividing n. For the sake of contradiction, assume p divides n exactly k times. We want to show that $k = 1$.

Let g be a primitive root modulo p^k. Then, $\gcd(a, p^k) = 1$. By hypothesis, we have

$$g^{n-1} \equiv 1 \pmod{n} \implies g^{n-1} \equiv 1 \pmod{p^k}.$$

Since g is a primitive root mod p^k, it has order $\phi(p^k) = p^{k-1}(p-1)$. And so $p^{k-1}(p-1)$ divides $n-1$. But $\gcd(p, n-1) = 1$ as $p \mid n$. This implies that $k = 1$ and $(p-1) \mid (n-1)$.

"This implies.." here is a bit handwavery. But the argument is identical to when proving Carmichael numbers are squarefree and the second half of Korselt's criterion.

Since p was arbitrary, we have shown that (1) and (2) of Korselt's criterion hold and so n is a Carmicheal number. ■

Proposition 6.10. Every Carmichael number has at least three prime factors.

Proof. Let n be a Carmichael number. Then n cannot have just one prime factor, because it is composite, and is the product of distinct primes. So, assume $n = pq$ where p, q are prime and $p > q$. Then

$$n - 1 = pq - 1 \equiv (p-1)q + (q-1) \equiv q - 1 \neq 0 \pmod{p-1}$$

which shows that $p-1$ does not divide $n-1$. Accordingly, n cannot be a Carmichael number. ■

7 Quadratic Residues

7.1 Did you mean quadratic equations?

We move on to quadratic residues. This is basically solving a quadratic equation but now solutions are only valid in $\mathbb{Z}$ (or rather in $\mathbb{Z}_n$). The goal of this section is to tackle the following problem.

"If p is a prime, $a \in \mathbb{Z}$. When does $x^2 \equiv a \pmod{p}$ has solutions?"

This seems like a natural question to ask considering its appearance in a number of our problems before. Before we start, let's make some observations.

(1). If $p = 2$, then we can always solve $x^2 \equiv a \pmod{p}$ as a can either be 0 or 1.

(2). If $p \mid a$, then $a \equiv 0 \pmod{p}$. It is again trivial that $x^2 \equiv a \pmod{p}$ is solvable ($x = 0$ does the job).

The conclusion is that we will now focus on the case that **p is odd** and **a coprime to p**. Let's begin with some definitions.

Definition 7.1. Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. We say that a is a **quadratic residue modulo p** if the congruence equation $x^2 \equiv a \pmod{p}$ has a solution.

If otherwise, we will say **a is a quadratic non-residue modulo p**.

We will sometimes write it as QR (quadratic residue) mod p or QNR (quadratic non-residue) mod p for brevity.

Remark. Being a QR depends only on the congruence class. Thus, it makes sense to ask if a congruence class $[a] \in \mathbb{Z}_p^\times$ is a QR or not. In other words:

If $a \equiv b \pmod{p}$, then a is a QR mod $p \iff b$ is a QR mod p.

Example. The QR mod 11 are the congruence classes 1, 3, 4, 5, 9.

We will now prove that only the even powers of a PR (primitive root) modulo p are QR mod p.

Lemma 7.1. Let $g \in \mathbb{Z}$ be a primitive root modulo p. Then, g^i is a quadratic residue modulo p *if and only if* i is even.

One sneaky observation that we can make is embedded in the following slogan

Slogan. A PR mod p is always a QNR mod p

This is because when $i = 1$ (which is odd) then g^i is... g.

Proof. ($\impliedby$). If i is even, then write $i = 2k$ for some $k \in \mathbb{Z}$. Then, we have $g^i = (g^k)^2$. Thus $x = g^k$ solves $x^2 \equiv g^i \pmod{p}$ i.e. g^i is a QR mod p.

($\implies$). Fix $i \geqslant 0$. Assume g^i is a QR mod p, then there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv g^i \pmod{p}$. Then, we have $x \equiv g^\alpha \pmod{p}$ for some $\alpha \in \mathbb{Z}$. So, $(g^\alpha)^2 \equiv x^2 \equiv g^i \pmod{p}$. Hence, we have that $2\alpha \equiv i \pmod{p-1}$. This is solvable if and only if $\gcd(2, p-1) = 2$ divides i. So i must be even. ∎

A nice corollary to this is the fact that half of the integers in any complete residue system modulo p are QR mod p and the other half being QNR mod p.

Proposition 7.1. There are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues in $\mathbb{Z}_p^\times$

Proof. Let g be a PR mod p. Then, we have $\mathbb{Z}_p^\times = \{[1], [g], [g]^2, \ldots, [g]^{p-2}\}$. By the previous lemma the QR are those with even powers of g^i i.e. $\{[1], [g]^2, \ldots, [g]^{p-3}\}$ and hence the QNR are those with odd powers of g^i i.e. $\{[g], [g]^3, \ldots, [g]^{p-2}\}$. Both sets contain $(p-1)/2$ elements. ∎

Corollary 7.1. (Euler's Criterion). Let $[a] \in \mathbb{Z}_p^\times$. Then $[a]$ is a QR mod p if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

and $[a]$ is a QNR mod p if and only if

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

Proof. Let g be a primitive root and suppose $[a] = [g]^i$. Then, $[a]^{(p-1)/2} = [g]^{i(p-1)/2}$ i.e. $(p-1)/2 \equiv i(p-1)/2 \pmod{p-1}$. Now, we have two cases.

i is even. If i is even, then we have $i(p-1)/2 \equiv 0 \pmod{p-1}$ which implies[17] $[g]^{i(p-1)/2} = [1] \implies [a]^{(p-1)/2} = [1]$.

i is odd. If i is odd, then we have[18] $i(p-1)/2 \equiv (p-1)/2 \pmod{p-1}$ which implies $[g]^{i(p-1)/2} = [g]^{(p-1)/2} = [-1] \implies [a]^{(p-1)/2} = [-1]$.

Recalling that even powers of a primitive root are quadratic residues completes the proof. ∎

[17] *as if g is a PR mod m, $g^i \equiv g^j \pmod{m} \iff i \equiv j \pmod{\phi(m)}$*

[18] *if i is odd, $i(p-1)/2 = k(p-1) + (p-1)/2 \equiv (p-1)/2 \pmod{p-1}$ for some $k \in \mathbb{Z}$.*

Corollary 7.2. Suppose p is a prime of the form $2^m + 1$ where $m \in \mathbb{N}$. Let $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$. Then

$$a \text{ is a primitive root mod } p \iff a \text{ is not a QR mod } p.$$

Proof. Since $\phi(p) = 2^m$ and the only prime divisor of 2^m is 2, the Primitive Root Test tells us that a is a primitive root mod p iff

$$a^{2^{m-1}} \not\equiv 1 \pmod{p}.$$

But observe that $(p-1)/2 = 2^{m-1}$. So by Euler's criterion, the above holds iff a is not a QR mod p. ∎

This theorem will seems to be out of nowhere but its usefulness will come later.

Theorem 7.2. (First Supplementary Law).

(1). $p \equiv 1 \pmod{4} \iff -1$ is a QR mod p.

(2). $p \equiv 3 \pmod{4} \iff -1$ is a QNR mod p.

Proof. Let g be a PR mod p, and consider $x = g^{\phi(p)/2} = g^{(p-1)/2}$. We have

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

where the last equality is because[19] g being PR mod p. The equation $x^2 \equiv 1 \pmod{p}$ has only two solutions (by Euclid's Lemma) either 1 or -1. But, $x \not\equiv 1 \pmod{p}$ (otherwise this contradicts primitivity of g). So, we must have $x \equiv -1 \pmod{p}$, i.e. $g^{(p-1)/2} \equiv -1 \pmod{p}$.

Now, by Lemma (7.1), -1 is a QR if and only if $(p-1)/2$ is even i.e. if $p \equiv 1 \pmod{4}$. On the other hand, -1 is a QNR if and only if $(p-1)/2$ is odd i.e. if $p \equiv 3 \pmod{4}$. ■

[19] *in particular, it has order* $\phi(p) = p - 1$

A very nice corollary to this theorem is the following fact.

Corollary 7.3. There are infinitely many primes p with $p \equiv 1 \pmod{4}$.

Proof. Suppose there are only finitely many primes p with $p \equiv 1 \pmod{4}$ such that $p \leqslant N$ where N is a positive integer. Consider $n = (N!)^2 + 1$, an odd integer. and let p be a prime divisor of n.

Now, $N!$ is divisible by every prime number which is $\equiv 1 \pmod{4}$. So, $(N!)^2 + 1$ is not divisible by any of these primes. But p has to be odd, so the only choice of p dividing n are those with $p \equiv 3 \pmod{4}$.

But then, since p divides n, we have $(N!)^2 \equiv -1 \pmod{p}$. -1 being a QR mod p but $p \equiv 3 \pmod{4}$? Sounds like a horror movie. Contradiction! ■

N is $\geqslant$ to **every** prime $\equiv 1 \pmod{4}$. So $N!$ must be a product of all of these primes i.e. $N!$ is divisible by all of these primes. But since $N \geqslant p$ for all $p \equiv 1 \pmod{4}$, if we square $N!$ and add 1, it is not divisible by any of these primes anymore. For example, say $N! = pq$ where p, q some primes. Then $n = (N!)^2 + 1 = p^2q^2 + 1$. If $p|n$ and since $p|p^2q^2$, we would have $p|1$ which is absurd! Similarly for q. So if there is a prime divisor of n, it better not be p, q or maths is broken.

Turns out that this result is a special case of a more general theorem — Dirichlet's Theorem.

Theorem 7.3. (Dirichlet's Theorem). Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. Then, there exists infinitely many primes p with $p \equiv a \pmod{b}$.

Proof. Suppose there are only finitely many primes p with $p \equiv$ okay I'm just joking. We're not proving this. ■

The proof of this theorem requires analytic number theory which is cool and cancerous at the same time. Come write a proof after you finish your Masters degree.

Proposition 7.2. Let p be an odd prime, and let a be a primitive root modulo p. Then

$$p - a \text{ is a primitive root modulo } p \iff p \equiv 1 \pmod{4}.$$

Proof. ($\implies$). If $p = 2$, the case is trivial. Suppose $p \equiv 3 \pmod{4}$. Then -1 is a QNR mod p. Since a is a primitive root mod p, a is also a QNR mod p. As the product of two QNR-s mod p is a QR, we must have $-a$ to be a QR mod p and therefore cannot be primitive. But observe that $p - a \equiv -a \pmod{p}$, so $p - a$ cannot be a primitive root mod p.

($\impliedby$). Suppose $p \equiv 1 \pmod{4}$. It is sufficient to show that $-a$ is a primitive root mod p as $p - a \equiv a \pmod{p}$.

Write $p = 1 + 4k$ for some $k \in \mathbb{Z}$. Then $\phi(p) = p - 1 = 4k$. By the Primitive Root Test, x is a primitive root mod p if and only if

$$x^{4k/q} \equiv 1 \pmod{p} \qquad (*)$$

for all prime divisors q of $4k$. If $q = 2$, then

$$(-x)^{4k/q} = (-x)^{2k} = x^{2k} \not\equiv 1 \pmod{p}$$

where the final non-equivalence is by $(*)$. Now if q is odd, then

$$(-x)^{4k/q} = (-x)^{4(k/q)} = x^{4(k/q)} \not\equiv 1 \pmod{p}$$

where the final non-equivalence is again by $(*)$. By the Primitive Root Test, $-x$ is thus a primitive root mod p. ∎

7.2 Legendre symbol

We now introduce a new notation that would be immensely helpful to keep track of quadratic residues (and later on, to even tackle problems related to them).

Definition 7.2. (Legendre Symbol). Let p be an odd prime, $a \in \mathbb{Z}$. We define the **Legendre symbol** $\left(\frac{a}{p}\right)$ by,

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } a \text{ is a QR mod } p \\ -1, & \text{if } a \text{ is a QNR mod } p \end{cases}$$

If $p \mid a$, we define $\left(\frac{a}{p}\right) = 0$.

Remark. The definition of the Legendre symbol depends only on the congruence class of a, so we can see it as being defined on elements $[a] \in \mathbb{Z}_p$. In other words, we can write $\left(\frac{a}{p}\right)$ as $\left(\frac{[a]_p}{p}\right)$.

One can also view the Legendre symbols as a map (in fact, a group homomorphism), $\left(\frac{\cdot}{p}\right) : [a]_p \mapsto \{-1, 0, 1\}$ where p here is fixed. What we want to do now is fix some p prime and take any a, then compute $\left(\frac{a}{p}\right)$. Why, because by definition of the Legendre symbol we have

$$\left(\frac{a}{p}\right) = 1 \iff x^2 \equiv a \pmod{p} \text{ has a solution}$$

This is also equivalent to saying that the QR mod p lives in the kernel of this map. The first thing that we will do now is reformulate Euler's Criterion (Corollary 7.1) using Legendre symbol.

Remark. (Euler's Criterion II.) Let $[a] \in \mathbb{Z}_p^\times$, then we have

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

In fact, if $p|a$, this is also true because both sides will just be 0 mod p.

Moreover, we also have another corollary to Lemma (7.1).

Corollary 7.4. (to Lemma 7.1). Let $g \in \mathbb{Z}$ be a primitive root mod p. Then.

$$\left(\frac{g^i}{p}\right) = (-1)^i \text{ for all } i \in \mathbb{N}$$

Proof. Let $i \in \mathbb{N}$. Then $\left(\frac{g^i}{p}\right) = 1 \iff g^i$ is a QR mod p. By Lemma (7.1), this is true if and only if i is even. By the same argument, we also have $\left(\frac{g^i}{p}\right) = -1 \iff i$ is odd. The claim follows. ■

Exercise. Use this corollary to prove Euler's Criterion in it's Legendre symbol form i.e. the remark above.

Lemma 7.4. Let p be an odd prime and $a, b \in \mathbb{Z}$ both coprime to p. Then

(1). $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

(3). $\left(\frac{1}{p}\right) = 1$

Proof. We have three things to proof.

(1). By a remark earlier after defining quadratic residues, we have that $a \equiv b \pmod{p}$ implies that a is a QR mod p if and only b is a QR mod p i.e. $\left(\frac{a}{p}\right) = 1 \iff \left(\frac{b}{p}\right) = 1$. Likewise, if it is a QNR.

(2). This is trivial. The equation $x^2 \equiv a^2 \pmod{p}$ has the very obvious solution $x = a$. So it must be a QR.

(3). Follows from (2) because $1 = 1^2$. ■

Lemma 7.5. There are $1 + \left(\frac{a}{p}\right)$ solutions in $\mathbb{Z}_p$ to the equation $x^2 \equiv a \pmod{p}$.

Remark. $1 + \left(\frac{a}{p}\right) \in \{0, 1, 2\}$. If QNR then 0. If p dividing a, then 1. If QR then 2.

Proof. Three cases to take care.

Case I. If $p \mid a$, then $x = [0]$ is the only single solution. So $1 = 1 + 0 = 1 + \left(\frac{a}{p}\right)$.

Case II. If a is a QNR mod p, then there are no solutions to the equation by definition of a non-residue. Also, $\left(\frac{a}{p}\right) = -1$. Indeed, $0 = 1 - 1 = 1 + \left(\frac{a}{p}\right)$.

Case III. If a is a QR mod p, then we have[20] two solutions, say λ and $-\lambda$. Now, by Lagrange's Theorem for polynomials mod p, the polynomial $x^2 - a$ has at most 2 solutions. So $\pm\lambda$ are all the solutions. Indeed, $2 = 1 + 1 = 1 + \left(\frac{a}{p}\right)$. ■

[20] *because $p > 2$ and $\lambda \neq [0]$, we must have that $\lambda \neq -\lambda$. Just pick any prime and choose any two numbers to see.*

Proposition 7.3. Let p be an odd prime and consider the quadratic equation

$$x^2 + bx + c \equiv 0 \pmod{p}$$

Then, the number of solutions to this equation in $\mathbb{Z}_p$ is

$$\left(\frac{\Delta}{p}\right) + 1$$

where $\Delta = b^2 - 4c$.

Remark. Our conclusion is equivalent to saying that the number of solutions in $\mathbb{Z}_p$ is

(1). 0 if $b^2 - 4c$ is a QNR mod p

(2). 1 if $b^2 - 4c \equiv 0 \bmod p$

(3). 2 if $b^2 - 4c$ is a QR mod p

Proof. The idea of the proof is — completing the square. We have that $x^2+bx+c \equiv 0 \pmod p$. Now, multiply by 4 on both sides, we have:

$$4x^2 + 4bx + 4c \equiv 0 \pmod p$$

Adding $b^2 - b^2$, we have

$$(4x^2 + 4bx + b^2) - b^2 + 4c \equiv 0 \pmod p$$

which implies

$$(4x^2 + 4bx + b^2) \equiv b^2 - 4c \pmod p$$

Letting $\Delta := b^2 - 4c$ and putting $4x^2 + 4bx + b^2$ into a square we have

$$(2x + b)^2 \equiv \Delta \pmod p$$

Now, by Lemma (7.5), the number of solutions to this equation is

$$\left(\frac{\Delta}{p}\right) + 1$$

■

Of course, calculations wouldn't be as efficient now. However, we promise you that it will get super efficient once we are done with the Second Supplementary Law and the Quadratic Reciprocity Law.

Lemma 7.6. (Legendre symbol is completely multiplicative). Let $a, b \in \mathbb{Z}$. Then

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

Proof. By Euler's Criterion II, we have

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

Since $p > 2$, both sides are either $1, 0$ or -1 so they must be equal. ■

In mod 2, you have $1 \equiv -1 \pmod 2$, so we REALLY need $p > 2$ for equality to happen.

Remark. A sneaky observation is that: (i) QNR × QNR = QR, (ii) QR × QNR = QNR, (iii) QR × QR. Of course these are facts that you don't need to memorize.

Remark. One **important** remark is the fact that

$$\left(\frac{-a}{p}\right) \not\Rightarrow -\left(\frac{a}{p}\right)$$

This is not always true! What is true is by using the Lemma above.

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \begin{cases} \left(\frac{a}{p}\right) & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{a}{p}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

With this knowledge of Legendre symbol being multiplicative, we can also state the following proposition.

Proposition 7.4. Let p be an odd prime. Then $[a] \in \mathbb{Z}_p^\times$ is a QR *if and only if* $[a]^{-1}$ is a QR.

Proof. By the multiplicativity of Legendre symbol, we have

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

So, if a is a QR mod p then this forces a^{-1} to be a QR mod p and vice-versa. ■

Exercise. Proof this directly using Euler's Criterion. You may want to use proof by contradiction.

Lemma 7.7.

$$\sum_{[a]\in\mathbb{Z}_p} \left(\frac{a}{p}\right) = 0$$

Note that we run $[a]$ over $\mathbb{Z}_p$ and not its multiplicative group. The argument of the proof still works very similarly.

Proof. There are altogether p elements in $\mathbb{Z}_p$. $(p-1)/2$ of them are QRs, $(p-1)/2$ of them are QNRs and one element, $[0]$ which is divisible by p — so this has $\left(\frac{0}{p}\right) = 0$. In total,

$$\frac{p-1}{2}(1) + \frac{p-1}{2}(-1) + 0 = 0$$

■

7.3 Sum of Squares modulo p

We have found and develop some interesting stuffs when answering the question whether a square modulo a prime has solutions or not. Let's go the extra mile and ask when and how many solutions does sum of squares modulo a prime has. We pose our problem more precisely below.

"Let $n \in \mathbb{N}$. How many solutions $(x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ does the equation $x_1^2 + x_2^2 + \ldots + x_n^2 \equiv 1 \pmod p$" have?

Definition 7.3. Let $n \in \mathbb{N}$. Then we define $N_n(p, a)$ or just $N_n(p)$ to be the number of solutions to the equation

$$x_1^2 + x_2^2 + \ldots + x_n^2 \equiv a \pmod p$$

Example. If $n = 1$, then the number of solutions to the equation $x_1^2 \equiv 1 \pmod p$ as seen earlier is 2, so $N_1(p, 1) = 2$.

Remark. In this notation we can also rewrite Lemma (7.5) as $N_1(p, a) = 1 + \left(\frac{a}{p}\right)$.

By the above remark, we are done with the general case when $n = 1$. Now, we deal with the case $n = 2$ i.e. a sum of two squares.

Example. Consider $p = 5, a = 1$. Then what is the number of solutions to the equation $x_1^2 + x_2^2 \equiv 1 \pmod 5$? Equivalently, what is $N_2(5, 1)$?.

Well there are 25 possibilities for $([x_1]_5, [x_2]_5) \in \mathbb{Z}_5^2$. We can list all of them and find the solutions by brute force. But that's not very efficient to do by hand. Here's a better strategy.

Step I. Suppose we have $y, z \in \mathbb{Z}_5$ with $y + z = [1]_5$, so we can write $y = [1]_5 - z$.

Step II. Solve $x_1^2 \equiv y \pmod 5$ and $x_2^2 \equiv z \equiv 1 - y \pmod 5$ separately. This would mean our Step I is just solving $x_1^2 + x_2^2 \equiv 1 \pmod 5$ as wanted!

Now these are just solving the case $n = 1$ again. We know how many solutions they have by Lemma (7.5)! $N_1(5, y) = 1 + \left(\frac{y}{5}\right)$ and $N_1(5, 1 - y) = 1 + \left(\frac{1-y}{5}\right)$.

Step III. We then get the total number of solutions to be:

$$\sum_{y \in \mathbb{Z}_5} N_1(5, y) \cdot N_1(5, 1 - y) = \sum_{y \in \mathbb{Z}_5} \left(1 + \left(\frac{y}{5}\right)\right)\left(1 + \left(\frac{1-y}{5}\right)\right)$$

Since when $y = 2, 3, 4$ we have $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{-3}{5}\right) = -1$. This is equals to

$$\underbrace{\left(1 + \left(\frac{0}{5}\right)\right)\left(1 + \left(\frac{1}{5}\right)\right)}_{y=0} + \underbrace{\left(1 + \left(\frac{1}{5}\right)\right)\left(1 + \left(\frac{0}{5}\right)\right)}_{y=1} + 0 + 0 + 0 = 4$$

So there are 4 solutions to $x_1^2 + x_2^2 \equiv 1 \pmod 5$, in other words $N_2(5, 1) = 4$. The solutions appear when $x_1^2 \equiv 0, 1 \pmod 5$. If $x_1 \equiv 0 \pmod 5$, then $x_2 \equiv \pm 1 \pmod 5$ and vice-versa. We have $(0, 1), (0, -1), (1, 0), (-1, 0)$ being all the solutions $\pmod 5$ and there are 4 of them as expected.

Let's try to generalize this.

Theorem 7.8. Let $a \in \mathbb{Z}$ and p be an odd prime. The equation $x_1^2 + x_2^2 \equiv a \pmod p$ has solutions (in $\mathbb{Z}_p \times \mathbb{Z}_p$)

$$N_2(p, a) = \begin{cases} p - \left(\frac{-1}{p}\right) & \text{if } p \nmid a \\ p + (p-1)\left(\frac{-1}{p}\right) & \text{if } p \mid a \end{cases}$$

Example. Using this formula, we get $N_2(5, 1) = 5 - \left(\frac{-1}{5}\right) = 4$ because $5 \equiv 1 \pmod 4$, so -1 is a QR mod 5. Most importantly, we get the same result as we had before.

Proof. The proof may seem complicated but it is not. For ease, we will list it down in steps. In fact, the steps are identical to the example above. Our goal is to find the number of solutions to $x_1^2 + x_2^2 \equiv a \pmod p$.

Step I. Suppose we have $y, z \in \mathbb{Z}_p$ with $y + z = [a]_p$, so we can write $y = [a]_p - z$.

Step II. Solve $x_1^2 \equiv y \pmod p$ and $x_2^2 \equiv z \equiv a - y \pmod p$ separately.

Step III. We then get the total number of solutions to be:

$$\begin{aligned} N_2(p,a) &= \sum_{y\in\mathbb{Z}_p} N_1(p,y)\cdot N_1(5,a-y) \\ &= \sum_{y\in\mathbb{Z}_p} \left(1+\left(\frac{y}{p}\right)\right)\left(1+\left(\frac{a-y}{p}\right)\right) \\ &= \sum_{y\in\mathbb{Z}_p} 1+\left(\frac{y}{p}\right)+\left(\frac{a-y}{p}\right)+\left(\frac{ay-y^2}{p}\right) \\ &= \sum_{y\in\mathbb{Z}_p} 1+\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right)+\sum_{y\in\mathbb{Z}_p}\left(\frac{a-y}{p}\right)+\sum_{y\in\mathbb{Z}_p}\left(\frac{ay-y^2}{p}\right) \end{aligned}$$

Let's evaluate the sums separately. The **first sum** is easy, we are just counting the number of congruence classes in $\mathbb{Z}_p$ and there are p of them.

$$\sum_{y\in\mathbb{Z}_p} 1 = p$$

The **second and third sum** dies by Lemma (7.7). So we have

$$\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right) = \sum_{y\in\mathbb{Z}_p}\left(\frac{a-y}{p}\right) = 0$$

to see how the third sum dies, think about the fact that as y runs over $\mathbb{Z}_p$, then $a-y$ also does so there is a bijection (think about it as *renaming*) $y \mapsto a-y$. Thus Lemma (7.7) applies.

Now, the **fourth sum** requires some thought. The trick is to realize that

$$ay - y^2 = y^2\left(\frac{a}{y}-1\right)$$

where "$1/y$" would make sense when $y \in \mathbb{Z}_p^\times$ which we will then write as $[y]_p^{-1}$. Using this trick, we can use multiplicativity of the Legendre symbol and try to separate[21] $\mathbb{Z}_p^\times$ from $\mathbb{Z}_p$.

[21] *but this is trivially easy because in mod p, we only need to remove* $[0]_p$ *and we are done.*

$$\begin{aligned} \sum_{y\in\mathbb{Z}_p}\left(\frac{ay-y^2}{p}\right) &= \left(\frac{0}{p}\right)+\sum_{y\in\mathbb{Z}_p^\times}\left(\frac{ay-y^2}{p}\right) \\ &= 0+\sum_{y\in\mathbb{Z}_p^\times}\left(\frac{y^2}{p}\right)\left(\frac{a[y]_p^{-1}-1}{p}\right) \\ &= \sum_{y\in\mathbb{Z}_p^\times}\left(\frac{a[y]_p^{-1}-1}{p}\right) \end{aligned}$$

where in the first equality $\left(\frac{0}{p}\right) = 0$ and in the last equality, $\left(\frac{y^2}{p}\right) = 1$. Now we have two cases.

Case 1: $p \mid a$**.** If $a \equiv 0 \pmod p$. Then, $a[y]_p^{-1} - 1 \equiv -1 \pmod p$. So, $\left(\frac{a[y]_p^{-1}-1}{p}\right) = \left(\frac{-1}{p}\right)$ by Lemma (7.4). It follows that:

$$\sum_{y\in\mathbb{Z}_p^\times}\left(\frac{a[y]_p^{-1}-1}{p}\right) = \sum_{y\in\mathbb{Z}_p^\times}\left(\frac{-1}{p}\right) = (p-1)\left(\frac{-1}{p}\right)$$

Case 2: $p \nmid a$**.** If $a \not\equiv 0 \pmod p$. Similar argument as in a margin note before, as

y runs over $\mathbb{Z}_p^\times$, then $a[y]_p^{-1}$ also runs over $\mathbb{Z}_p^\times$. In other words, there is a bijection $y \mapsto a[y]_p^{-1}$ (so we can just *rename* everything). Let's *rename* $a[y]_p^{-1}$ to be b. Then,

pay attention to whether $b \in \mathbb{Z}_p^\times$ or $b \in \mathbb{Z}_p$.

$$\begin{aligned}\sum_{y\in\mathbb{Z}_p^\times}\left(\frac{a[y]_p^{-1}-1}{p}\right) &= \sum_{b\in\mathbb{Z}_p^\times}\left(\frac{b-1}{p}\right)\\ &= \underbrace{\left(\frac{0}{p}\right)+\left(\frac{1}{p}\right)+\cdots+\left(\frac{p-2}{p}\right)}_{p-1 \text{ terms}}\\ &= \underbrace{\left(\sum_{b\in\mathbb{Z}_p}\left(\frac{a}{p}\right)\right)}_{p \text{ terms}}-\left(\frac{p-1}{p}\right)\\ &= -\left(\frac{p-1}{p}\right)\\ &= -\left(\frac{-1}{p}\right)\end{aligned}$$

where $\sum_{b\in\mathbb{Z}_p}\left(\frac{a}{p}\right) = 0$ by Lemma (7.7). So, summing the first and the fourth sum (which have two cases), we get our claim. ∎

Now, we know how many solutions to expect to the sum of two squares of modulo p. In particular, we know how many solutions to the equation $x_1^2 + x_2^2 \equiv 1 \pmod p$. There are $N_2(p, 1)$ solutions. But what do the solutions look like?

Example. We will look at some cases.

Example I: $p = 5$. Then we had in the previous example that the solutions are $\{(1,0),(0,1),(-1,0),(0,-1)\}$ and there are 4 them.

Example II: $p = 7$. Now here, we use the formula that we had just found to see that we should expect $N_2(7,1) = 7 - \left(\frac{-1}{7}\right) = 8$ solutions. What are they? Well, we had the same $\{(1,0),(0,1),(-1,0),(0,-1)\}$, so there are 4 of them here. Then, we also have $\{(2,2),(-2,2),(2,-2),(-2,-2)\}$, there are also 4 of them here.

Example II: $p = 11$. We have $N_2(11,1) = 11 - \left(\frac{-1}{11}\right) = 12$ solutions. Again, we have $\{(1,0),(0,1),(-1,0),(0,-1)\}$ as solutions. We have the other 8 in here $\{(\pm 3,5),(\pm 3,-5),(5,\pm 3),(-5,\pm 3)\}$.

Can you spot the pattern? Observe how these solutions come in *packages*. If you have a pair of solution, then you *usually can*[22] get other 7 pairs for free by swapping entries and changing signs. This also shows how the $N_2(p,a)$ formula is useful. It tells you when to stop brute-forcing.

[22] *the set of solutions* $\{(\pm 1,0),(0,\pm 1)\}$ *have only 4 elements because you can't consider plus-minus* 0. *On the other hand, the set of solutions* $\{(2,2),(-2,2),(2,-2),(-2,-2)\}$ *have only 4 elements because the first entry and the second entry are the same number up to a sign.*

Using this idea, we can get a nice corollary that would be extremely useful when computing QR mod p.

Corollary 7.5. (Second Supplementary Law). Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases}+1 & \text{if } p \equiv \pm 1 \pmod 8\\ -1 & \text{if } p \equiv \pm 3 \pmod 8\end{cases}$$

Proof. The idea is to count the number of solutions to $x_1^2 + x_2^2 \equiv 1 \pmod{p}$ in two different ways.

First way. We had the formula, $N_2(p,1) = p - \left(\frac{-1}{p}\right)$

Second way. As in the example, we see that solutions come in *packages* — get one pair, then (possibly) get 7 pairs by swapping and changing signs. Suppose we have a solution (x,y). Then, these are all solutions as well

$$(y,x),\ (-x,y),\ (x,-y),\ (-x,-y),\ (-y,x),\ (y,-x),\ (-y,-x)$$

In total, a single solution *usually* gives 8 distinct solutions (including itself). When don't we get 8 distinct solutions then? Well there would be two reasons.

1. Changing signs does not change signs — this happens when x or $y = 0$.
2. Swapping does not swaps — this happens when $x = \pm y$.

Case 1. If $x = 0$, then $y = \pm 1$ for the pair to be a solution and likewise if $y = 0$, then $x = \pm 1$ for the pair to be a solution. So, we get 4 solutions.

Case 2. If $x = \pm y$, or equivalently we can put, if $(x,y) = (\lambda, \pm\lambda)$, then $\lambda^2 + \lambda^2 \equiv 1 \pmod{p}$ i.e. $2\lambda^2 \equiv 1 \pmod{p}$. We can rearrange this to have

$$\lambda^2 \equiv 2^{-1} \pmod{p} \qquad (*)$$

How many solutions do we have here? Well there are $N_1(p, 2^{-1}) = 1 + \left(\frac{[2]_p^{-1}}{p}\right)$ solutions. Since a is a QR mod p iff a^{-1} is a QR mod p by Proposition (7.4), we thus have

$$N_1(p, 2^{-1}) = 1 + \left(\frac{2}{p}\right)$$

We thus have **2 subcases to consider**. If $\left(\frac{2}{p}\right) = -1$, there are no solutions to $(*)$. If $\left(\frac{2}{p}\right) = 1$, there are 2 solutions to $(*)$ and hence, 4 solutions overall since we could have $-\lambda$ as well.

there are 2 possibilities for λ and hence there are 4 possibilities for $(\lambda, \pm\lambda)$ (consider swapping as well!)

The conclusion. Therefore, in total we have:

$$\begin{aligned} N_2(p,1) &= 8 \times \left(\begin{smallmatrix}\text{Number of } \textit{packages} \text{ that} \\ \text{leads to 8 distinct solutions}\end{smallmatrix}\right) + \text{ Case 1 solutions } + \text{ Case 2 solutions} \\ &= 8k + 0 + \underbrace{1 + \left(\frac{2}{p}\right)}_{\text{either 0 or 4}} \end{aligned}$$

where $k \in \mathbb{Z}$ (we will see it doesn't really matter below). In particular, we can just write this as

$$N_2(p,1) \equiv \begin{cases} 4 \pmod{8} & \text{if } \left(\frac{2}{p}\right) = -1 \\ 0 \pmod{8} & \text{if } \left(\frac{2}{p}\right) = 1 \end{cases}$$

See, the k vanishes, we only care that it is a multiple of 4. But from our first way of counting $N_2(p,1)$, we have that $N_2(p,1) = p - \left(\frac{-1}{p}\right)$. So we have that:

$$p - \left(\frac{-1}{p}\right) \equiv \begin{cases} 4 \pmod{8} & \text{if } \left(\frac{2}{p}\right) = -1 \qquad (£) \\ 0 \pmod{8} & \text{if } \left(\frac{2}{p}\right) = 1 \qquad (\dagger) \end{cases}$$

Now let's compare both sides. Since p is odd $p \equiv 1, 3, 5, 7 \pmod 8$ or equivalently, $p \equiv 1, 3, -3, -1 \pmod 8$. Now $p \equiv 1 \pmod 8$, iff $\left(\frac{-1}{p}\right) = 1$ (by Theorem 7.2) so this is the case of (†). Also, $p \equiv -1 \pmod 8$, iff $\left(\frac{1}{p}\right) = 1$, then this is also the case (†). We leave the reader to check that $p \equiv \pm 3 \pmod 8$ leads to the case of (£). ■

Remark. (When is 2 a QR mod p?)

(1). $p \equiv \pm 1 \pmod 8 \iff 2$ is a QR mod p.

(2). $p \equiv \pm 3 \pmod 8 \iff 2$ is a QNR mod p.

Recall that there's no easy way to find a primitive root other than brute force or inspection with luck. The following corollary would definitely save 5 minutes of your exam time by making you **not try** the most tried and most anticipated primitive root of all.

Corollary 7.6. If $p \equiv \pm 1 \pmod 8$, then 2 is not a primitive root modulo p.

Proof. Suppose for contradiction that 2 is a primitive root mod p. By Lemma (7.1), 2^i is a QR mod p if and only if i is even. In particular $i \neq 1$. Now, since $p \equiv \pm 1 \pmod 8$, the Second Supplementary Law tells us that 2 is a QR mod p [ϟ]. ■

Slogan. If $p \equiv \pm 1 \pmod 8$, then don't try 2 (as primitive root).

The following theorem gives us the precise number of solutions to the equation $x_1^2 + x_2^2 + \ldots x_n^2 \equiv 1 \pmod p$ when n is odd.

Theorem 7.9. Let $n = 2k + 1$ be an odd positive integer. Then

$$N_n(p, 1) = p^{2k} + p^k \left(\frac{-1}{p}\right)^k$$

Proof. We will not give a full proof. But the idea is that to first find $N_n(p, 1)$ in terms of $N_{n-2}(p, 1)$. Then, we prove by induction on k assuming the formula as in the theorem holds. ■

In a similar spirit, we can find a formula for $N_n(p, 1)$ for n even but we only truly care for when n is odd. This is because we can prove the Quadratic Reciprocity Law (coming next) just by computing $N_q(p, 1)$ in two different ways where p, q are odd distinct primes.

7.4 Quadratic Reciprocity

We arrive to the most important subsection, the Theorema Aureum, the Quadratic Reciprocity Law. This is a theorem of Gauss, first proven in 1796. Gauss gave eight stunning different proofs of this theorem. This is one of many jewel of mathematics. The proof that is given in lectures by Dr. Newton is due to V. Lebesgue which is done by thinking about the number of solutions $x_1^2 + x_2^2 + \ldots + x_q^2 \equiv 1 \pmod p$ in $\mathbb{Z}_p^q$ where q is an odd prime distinct from p. We know the number of solutions to this equation (by the previous theorem) to be $N_q(p, 1)$. Let's try to compute it in a different way, just like how we did when proving the Second Supplementary Law.

Theorem 7.10. (Quadratic Reciprocity Law). Let p, q be two distinct odd primes.

Then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Proof. Let p, q be distinct odd primes. Just like proving the Second Supplementary Law, we will now prove the theorem by computing $N_q(p, 1)$ in two different ways and comparing.

First way. By the previous theorem, we have a formula since q is odd. Write $q = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$N_q(p,1) = p^{q-1} + p^{\frac{q-1}{2}}\left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \equiv 1 + \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod q$$

$p^{q-1} \equiv 1 \pmod q$ by Fermat's little theorem; and $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$ and $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right)$ by Euler's criterion II.

Second way. Let's think about solutions (in $\mathbb{Z}_p^q$) to $x_1^2 + x_2^2 + \ldots + x_q^2 \equiv 1 \pmod p$ directly. Suppose we have one solution $(x_1, x_2, \ldots, x_q)$. Then, we can get q solutions (including the original one) by cyclic permutation.

we don't know if these q solutions are distinct yet!

$$(x_1, x_2, x_3, \ldots, x_{q-1}, x_q),\ (x_2, x_3, x_4, \ldots, x_q, x_1),\ \ldots,\ (x_q, x_1, x_2, \ldots, x_{q-2}, x_{q-1})$$

We then have two cases, either every entry equal, or every entry different (this is a claim!)

Case I. Now, suppose $x_1 = x_2 = \cdots = x_q$. So, $qx_1^2 \equiv 1 \pmod p$. Then, we get the same solutions q times. The number of solutions like this would then be:

e.g. Suppose $q \equiv 1 \pmod p$, example: $q = 11, p = 5$. Then $(1, 1, 1, \ldots, 1)$ and $(-1, -1, -1, \ldots, -1)$ are solutions (for the case $x_i = x_j$ for all $i \neq j$). And cyclic permutations does nothing.

$$\begin{cases} 0 & \text{if } [q]_p^{-1} \text{ is a QNR} \\ 2 & \text{if } [q]_p^{-1} \text{ is a QR} \end{cases} \overset{\text{(by Proposition 7.4)}}{\underset{\downarrow}{\iff}} \begin{cases} 0 & \text{if } [q]_p \text{ is a QNR} \\ 2 & \text{if } [q]_p \text{ is a QR} \end{cases} = 1 + \left(\frac{q}{p}\right)$$

Case II. We claim that if it is not Case I, then cyclic permutations always give q distinct solutions. The idea is to prove by contradiction — we assume the opposite, and then shows that if it is so, then it must be Case I. Let's start, suppose cyclic permutation doesn't give distinct solutions i.e. we have

$$(x_1, x_2, \ldots, x_q) = (x_i, x_{i+1}, \ldots, x_q, x_1, \ldots, x_{i-1})$$

for some $1 < i \leqslant q$. This says that

$$\begin{aligned} x_1 &= x_i \\ x_2 &= x_{i+1} = x_{2+(i-1)} \\ &\vdots \\ x_q &= x_{i-1} = x_{q+(i-1)} \end{aligned}$$

Interpret the suffix/subscript $q + (i - 1)$ as modulo q (stare at the equations long enough). The way we write it is just saying that the sequence of numbers $x_1, x_2, \ldots, x_n$ (which together forms a single set of solution $(x_1, x_2, \ldots, x_n)$) repeats with period $i - 1$.

Now, since $1 < i \leqslant q$, then $0 < i - 1 \leqslant q - 1$, so $i - 1$ is coprime to q. This means that there exists an integer which if we multiply by $i-1$, we get 1 modulo q i.e. there exists $k \in \mathbb{N}$, so that $(i-1)k \equiv 1 \pmod{q}$. And we said that the sequence repeats with period $i-1$, so think about what happens if we do this k times. We have

$$x_n = x_{n+(i-1)}, \forall n$$

but then we also have

$$x_{n+(i-1)} = x_{n+(i-1)+(i-1)}, \forall n$$

and so on. Repeating this k times (we choose the same k as before) we have

$$x_n = x_{n+(i-1)k} = x_{n+1}, \forall n$$

The last equality is due to the fact that $(i-1)k \equiv 1 \pmod{q}$ — recall that we interpret the suffix as modulo q.

But, then this just tells us that we repeat with period 1, so really all the numbers are the same. So we're back at Case 1. [↯]

Conclusion. Therefore, in total we have

$$\begin{aligned} N_q(p,1) &= q \times \left(\begin{smallmatrix}\text{Number of } \textit{packages} \text{ that} \\ \text{leads to } q \text{ distinct solutions}\end{smallmatrix}\right) + \text{ Case 1 solutions} \\ &= qr + 1 + \left(\frac{q}{p}\right) \\ &\equiv 1 + \left(\frac{q}{p}\right) \pmod{q} \end{aligned}$$

where $r \in \mathbb{Z}$ which doesn't really matter since it dies anyway when we consider mod q. Comparing the **First way** and the **Second way** we have the congruence

$$1 + \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv 1 + \left(\frac{q}{p}\right) \pmod{q}$$

which implies

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

But because $q > 2$ and both sides of the congruence are either 1 or -1, this further implies that to achieve congruence mod q, they actually have to be equal. Thus, we have

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

in mod 2, $1 \equiv -1$, so being congruent doesn't mean being equal. But modulo higher than 2, $1 \not\equiv -1$. So to achieve congruence mod $q > 2$ for numbers that could either be 1 or -1, they must be equal.

■

Corollary 7.7. Let p be an odd prime. Then

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Proof. Our main tools are the Quadratic Reciprocity Law and the Chinese Remainder Theorem. We will only prove that that if $p \equiv \pm 1 \pmod{12}$, then 3 is a QR mod p.

Case 1. If $p \equiv 1 \pmod 4$, then by the reciprocity law:

$$\left(\frac{3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1$$

Since the only QR mod 3 is $[1]_3$, we must have $p \equiv 1 \pmod 3$. By the CRT, we get $p \equiv 1 \pmod{12}$.

we don't include 0 as QR by our definition.

Case 2. If $p \equiv 3 \pmod 4$, then by the reciprocity law:

$$\left(\frac{3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = -1$$

Since the only QNR mod 3 is $[2]_3$, we must have $p \equiv 2 \pmod 3$. By the CRT, we get $p \equiv 11 \equiv -1 \pmod{12}$.

The claim follows. ■

Corollary 7.8. Let p, q be odd primes such that $p = q + 4a$ for some $a \in \mathbb{Z}$. Then,

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

Proof. The trick is to multiply both sides by $1 = \left(\frac{4}{p}\right) = \left(\frac{4}{q}\right)$. This turns our problem into proving $\left(\frac{4a}{p}\right) = \left(\frac{4a}{q}\right)$. Let's make some observations first. Given $p = q + 4a$, so we have:

1. $p \equiv q \pmod 4$
2. $p \equiv 4a \pmod q$
3. $-q \equiv 4a \pmod p$

Therefore, we have that

$$\text{LHS} = \left(\frac{4a}{p}\right) = \left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right)$$

We now have two cases two consider, whether -1 is a QR mod p or not.

Case I: -1 is QR. If -1 is QR, then $p \equiv q \equiv 1 \pmod 4$. Thus we have:

$$\text{LHS} = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right) \overset{\text{(QRL)}}{\downarrow} = \left(\frac{p}{q}\right) = \left(\frac{4a}{q}\right) = \text{RHS}$$

Case I: -1 is QNR. If -1 is QNR, then $p \equiv q \equiv 3 \pmod 4$.

$$\text{LHS} = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = -\left(\frac{q}{p}\right) \overset{\text{(QRL)}}{\downarrow} = -\left(-\left(\frac{p}{q}\right)\right) = \left(\frac{p}{q}\right) = \left(\frac{4a}{q}\right) = \text{RHS}$$

■

8 Sum of Squares

First, we define what does it mean to be a square.

Proposition 8.1. A positive integer n is a square *if and only if* **every** exponent a_i in the prime factorisation $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ is even.

Rather than attacking sum of 100 squares, it is only natural to start from the simplest condition and ask:

"*Which positive integers* are sum of two squares?"

Well, let's do it by inspection first. Write some positive integers. **1**, **2**, 3, **4**, **5**, 6, 7, **8**, **9**, **10**, 11, 12, **13**. Notice that the boldfaced letters are sums of two squares.

$$\begin{aligned} 1 &= 0^2 + 0^2 \\ 2 &= 1^2 + 1^2 \\ 4 &= 2^2 + 0^2 \\ 5 &= 2^2 + 1^2 \\ 8 &= 2^2 + 2^2 \\ 9 &= 3^2 + 0^2 \\ 10 &= 3^2 + 1^2 \\ 13 &= 3^2 + 2^2 \end{aligned}$$

Can you see the underlying pattern? Well it's not immediately obvious that's for sure.

Lemma 8.1. Suppose that $n = a^2 + b^2$, $a, b \in \mathbb{Z}$. Then $n \equiv 0, 1$ or $2 \pmod 4$.

Proof. Let's look at the squares mod 4. We have

$$\begin{aligned} 0^2 &\equiv 0 \pmod 4 \\ 1^2 &\equiv 1 \pmod 4 \\ 2^2 &\equiv 0 \pmod 4 \\ 3^2 &\equiv 1 \pmod 4 \end{aligned}$$

Since a square mod 4 can either be 0 or 1, it follows that a sum of two squares can only be either $0, 1$ or $2 \pmod 4$. ∎

Remark. The reverse direction is **not true**! Consider the number $1265 = 5 \cdot 11 \cdot 23$. Notice that $5 \equiv 1 \pmod 4$ and $11 \equiv 23 \equiv -1 \equiv 3 \pmod 4$. Therefore, we have $1265 \equiv 1 \cdot (-1) \cdot (-1) \equiv 1 \pmod 4$. But, 1265 is **not** a sum of two squares.

Corollary 8.1. If $n \equiv 3 \pmod 4$, then n is not a sum of two squares.

Proof. Take the contrapositive of the Lemma. ∎

Lemma 8.2. Let $m, n \in \mathbb{N}$. If m and n are sum of two squares, then so is mn.

Proof. Suppose $m = a^2 + b^2 = |a + ib|^2$ and $n = c^2 + d^2 = |c + id|^2$. Then,

$$mn = |a + ib|^2 |c + id|^2 = |(a + ib)(c + id)|^2 = |(ac - bd) + i(ad + bc)|^2$$

which is also a sum of two squares. ■

Aha! Knowing this fact, our initial question of asking which positive integers are sum of two squares reduces to asking

"*Which primes can be written as sum of two squares?*"

By Lemma (8.1), we get for free that if $p \equiv 3 \pmod 4$, then p is **not** a sum of two squares. So we are concern with the case that $p = 2$ and $p \equiv 1 \pmod 4$.

Theorem 8.3. Let p be a prime. Then, p is a sum of two squares *if and only if* $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. ($\implies$) If p is a sum of two squares, then $p = 2$ or $p \equiv 1 \pmod 4$ by Lemma (8.1).

($\impliedby$). Now $2 = 1^2 + 1^2$, so $p = 2$ is a sum of two squares. It remains to check that if $p \equiv 1 \pmod 4$ then it is a sum of two squares. The idea is to use the *pigeonhole principle*. Now, by the First Supplementary Law, $p \equiv 1 \pmod 4$ implies that -1 is a QR mod p. So, let $b \in \mathbb{Z}$ such that $b^2 \equiv -1 \pmod p$. Now, consider the number

$$k = \lfloor \sqrt{p} \rfloor$$

which is the biggest integer $\leqslant \sqrt{p}$. But p is a prime, so $\sqrt{p}$ is not an integer. So, we really have $k < \sqrt{p}$. Now, the point of considering this number is that we then have $k^2 < p < (k+1)^2$. We will see why this is at the heart of the proof below.

the pigenhole principles tells us that if you have m objects and n holes such that $m > n$, then at least one of the holes must contain more than 1 object.

because $k < \sqrt{p} < k + 1$

Consider the pairs of integers (c, d) with $0 \leqslant c \leqslant k$ and $0 \leqslant d \leqslant k$. There are $k + 1$ choices for c and $k + 1$ choices for d. In total, we have $(k + 1)^2$ choices to form pairs (c, d). Now, from any pair (c, d) construct an integer by the map

$$(c, d) \mapsto c + bd$$

where b is as defined earlier. Since there are $(k + 1)^2$ pairs (c, d), we have a list of $(k + 1)^2$ integers $c + bd$:

$$0, b, 1, 1 + b, 2, 2b, \ldots, k + bk$$

Now, since $(k + 1)^2 > p$ but there are only p distinct residue classes mod p, the pigeonhole principle tells us that

$$c_1 + bd_1 \equiv c_2 + bd_2 \pmod p$$

for some pair $(c_1, d_1) \neq (c_2, d_2)$. Thus,

$$c_1 - c_2 \equiv b(d_2 - d_1) \pmod p$$

Squaring both sides and recalling that $b^2 \equiv -1 \pmod p$, we have

$$(c_1 - c_2)^2 \equiv -1 \cdot (d_2 - d_1)^2 \pmod p$$

Thus,

$$(c_1 - c_2)^2 + (d_2 - d_1)^2 \equiv 0 \pmod p$$

We are really close to saying that p is a sum of two squares! We just need to check

that the LHS is not just congruent to 0 mod p i.e. p divides it, but indeed have to be equal to p. This is not too hard.

We know that $0 \leqslant c_1, c_2, d_1, d_2 \leqslant k$. So, we have that

$$0 \leqslant (c_1 - c_2)^2 \leqslant k^2 < p \quad \text{and} \quad 0 \leqslant (d_1 - d_2)^2 \leqslant k^2 < p$$

We can sum these together to have

$$0 \leqslant (c_1 - c_2)^2 + (d_1 - d_2)^2 < 2p$$

Let's have a think. What is an integer λ such that $p \mid \lambda$ and $0 \leqslant \lambda < 2p$? Well, the only possibilities are 0 and p. So the sum $(c_1 - c_2)^2 + (d_1 - d_2)^2$ can only be either 0 or p. The only way for it to be 0 is that if $c_1 = c_2$ and $d_1 = d_2$. But, $(c_1, d_1) \neq (c_2, d_2)$. So this forces the sum to be p and this is a sum of two squares. We are done now. ■

Remark. Another interesting example of the pigeonhole principle is that if there are 367 people in a room, then at least two of them share a birthday. The pigeonhole principle was also stated in a slightly different way in the subsection of Chinese Remainder Theorem (4.1). These are equivalent statements.

Remark. Combine this theorem with the previous lemma, we can conclude that the integer

$$2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

with primes $p_i \equiv 1 \pmod 4$ for all i is a sum of two squares.

Remark. Furthermore, if $m \in \mathbb{N}$, then $m^2 = 0^2 + m^2$. If $n \in \mathbb{N}$ is a sum of two squares, then $n = a^2 + b^2$. Multiplying we get that $m^2 n = (am)^2 + (bm)^2$ so $m^2 n$ is a sum of two squares. We conclude that for any $m \in \mathbb{N}$ and $p_1, p_2, \ldots, p_k \equiv 1 \pmod 4$ primes, the integer

$$m^2 \cdot 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

is a sum of two squares.

Proposition 8.2. If an integer is a sum of two squares, it must be of the form

$$m^2 \cdot 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \tag{8.1}$$

where $m \in \mathbb{N}$, $p_i \equiv 1 \pmod 4$ primes for all $1 \leqslant i \leqslant k$ and $a_i \geqslant 0$ for all $0 \leqslant i \leqslant k$.

Example. $104 = 8 \times 13 = 2^3 \times 13$ is a sum of two squares. Well, $8 = 2^2 + 2^2$ and $13 = 2^2 + 3^2$. We could rewrite this $8 = |2 + 2i|^2$ and $13 = |2 + 3i|^2$. So we have

$$104 = |(2 + 2i)(2 + 3i)|^2 = |4 + 6i + 4i - 6|^2 = |-2 + 10i|^2 = 2^2 + 10^2$$

Theorem 8.4. (Two Squares Theorem). $n \in \mathbb{N}$ is a sum of two squares *if and only if* the exponent of every prime number which is congruent to 3 mod 4 in the prime factorisation of n is even.

Proof. ($\Longleftarrow$). Suppose $n = m^2 p_1 p_2 \cdots p_k$ with each prime p_i being equal to either 2 or $\equiv 1 \pmod 4$ and $m \in \mathbb{N}$. Then p_i are all sum of two squares by Theorem (8.3). m^2 is also a sum of two squares also . Moreover, if the exponent of every prime number $\equiv 3 \pmod 4$ is even, then it must divide m^2. Now, by Lemma (8.2), we have that

$m^2 = 0^2 + m^2$ for any $m \in \mathbb{N}$

their product is a sum of two squares.

($\implies$). Suppose $n = a^2 + b^2$. We want to show that every prime $p \equiv 3 \pmod 4$ appears with an even power in the prime factorisation of n. Let's make things in a coprime setting. Let $d = \gcd(a, b)$. Then

$$n = d^2 \left(\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 \right)$$

where a/d and b/d are coprime. **Our goal is now to show that any prime $p \equiv 3 \pmod 4$ dividing n must divide d^2 only and not the second term.**

Suppose $p|n$ and $p \equiv 3 \pmod 4$. If p divides $\left(\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2\right)$, then

$$\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 \equiv 0 \pmod p \implies \left(\frac{a}{d}\right)^2 \equiv -\left(\frac{b}{d}\right)^2 \pmod p$$

Now since a/d and b/d are coprime, neither one of them is divisible by p. So we have

$$\left(\frac{a}{d}\right)^2 \left[\left(\frac{b}{d}\right)^2\right]_p^{-1} \equiv -1 \pmod p$$

which can be rewritten as

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

i.e. implying that -1 is a QR mod p. But $p \equiv 3 \pmod 4$, this contradicts the First Supplementary Law. So, p must divide d^2, the square term, we are done. ■

If, say, a/d is divisible by p, then the congruence would say that b/d is also divisible by p so p divides $\gcd(a/d, b/d) = 1$.

Combining the result from Proposition (8.2) and the Two Squares Theorem, we have that if $p \equiv 3 \pmod 4$ and it divides (8.1), then it must[23] divide m^2, and hence divides m. So, the power of $p \equiv 3 \pmod 4$ in the prime factorisation must be even.

[23] *and no others because the primes that pops up there are congruent to* 1 *mod* 4.

Corollary 8.2. Let $n \in \mathbb{N}$. If $n = x^2 + y^2$ with $x, y \in \mathbb{Q}$, then n is also a sum of two **integer** squares.

Proof. Exercise. ■

Theorem 8.5. (Three Squares Theorem). A positive integer is a sum of three squares *if and only if* it is **not** of the form $4^\alpha(8k + 7)$ where $\alpha, k \in \mathbb{N} \cup \{0\}$.

Proof. Omitted. One direction is not too bad, the other is super hard. ■

Example. Take $15 = 4^0(8 \cdot 1 + 7)$. This is not a sum of three squares.

Lemma 8.6. If m and n are sums of four squares, then the product mn is also a sum of four squares.

Proof. Exercise. ■

Theorem 8.7. (Four Squares Theorem, Lagrange 1770). Every positive integer is a sum of four squares.

Proof. Omitted, but uses the above lemma. ∎

8.1 A digression: Differences of two squares

Proposition 8.3. Suppose p is an odd prime of the form $p = a^2 - b^2$ for some positive integers $a, b \in \mathbb{N}$. Then

$$a = \frac{p+1}{2} \quad \text{and} \quad b = \frac{p-1}{2}$$

Proof. $p = a^2 - b^2 = (a-b)(a+b)$. Since p is prime and $a + b > a - b$, we must have $a - b = 1$ and $a + b = p$. Solving for a and b, we get our desired result. ∎

Theorem 8.8. Every positive **odd** integer $n > 1$ can be written as a difference of two squares.

Proof. We want to show that there exist $a, b \in \mathbb{N}$ such that $n = a^2 - b^2$. Well, consider

$$a = \frac{n+1}{2} \quad \text{and} \quad b = \frac{n-1}{2}$$

and we are done. ∎

PART

III

A useful digression

We will now dive into a world with a slightly different theme to what we have been discussing so far. This is where number theory starts to branch out into what we today call algebraic number theory and analytic number theory.

9 Irrational, Algebraic and Transcendental Numbers

9.1 Irrational Numbers

We first start by recalling some notations. By $\mathbb{Q}$, we mean the set of rational numbers $\{a/b : a \in \mathbb{Z}, b \in \mathbb{N}\}$. By $\mathbb{R}$, we mean the real numbers and by $\mathbb{C}$ we mean the set of complex numbers. Note that all three of these are actually fields.

Definition 9.1. A complex number $z \in \mathbb{C}$ is called **irrational** if $z \notin \mathbb{Q}$.

Notice that we **include** the complex numbers with non-zero imaginary part to be an irrational number as well!

Example. $\sqrt{2}$, $\sqrt{n}$ when $n \in \mathbb{N}$ is not a square, $\sqrt{-1} = i$, $2 + 3i$.

Theorem 9.1. A real number $x \in \mathbb{R}$ is **rational** *if and only if* its decimal expansion either terminates **or** repeats.

Example. $1/10 = 0.1$ terminates so it is rational. $1/9 = 0.1111...$ repeats so it is rational.

Proof. ($\Longleftarrow$). Suppose the decimal is eventually repeating or terminating. WLOG, suppose $0 < x < 1$. So, we can write $x = 0.\overline{a_1 a_2 a_3 \dots a_r}$. Then, we have

$$10^r x = a_1 a_2 \cdots a_r + x.$$

see remark below for explanation of this step

Thus, we have

$$x = \frac{a_1 a_2 \cdots a_r}{10^r - 1} \in \mathbb{Q}$$

($\Longrightarrow$). Exercise. ∎

Remark. We have

$$x = 0.\overline{a_1 a_2 a_3 \dots a_r} = a_1 \dots a_r a_1 \dots a_r \dots \text{repeats of } a_1 a_2 a_3 \dots a_r$$

Multiplying by 10 *shifts* x once (e.g. $x = 0.23$, then $10x = 2.3$). So, multiplying by 10^r *shifts* x by r times.

$$10^r x = \underbrace{a_1 \cdots a_r}_{\text{product of } a_i} . \underbrace{a_1 \dots a_r \dots \text{repeats of } a_1 a_2 a_3 \dots a_r}_{\text{decimal expansion with repeating } a_i} = a_1 a_2 a_3 \dots a_r + x$$

Example. Here are three examples of numbers being irrational because it doesn't satisfy the theorem above.

1. $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is irrational. If you expand this, you will see that the gap between a 1 and another 1 gets bigger as n gets larger (in between will be filled with a lot of zeroes). The decimal expansion does not repeat nor terminate.

2. $\beta = \sum_{n=1}^{\infty} \frac{1}{2^{n!}}$. For same reasons, this is irrational. Instead of looking at the decimal expansion, look at the binary expansion — there's nothing special about the number 10 in the statement of the theorem.

3. You can replace 10 and 2 in the above examples with any other positive integer and look at the expansion with respect to that base. For same reasons, this number will also be irrational.

Let's find more ways to find irrational numbers.

Proposition 9.1. Suppose $z \in \mathbb{C}$ is a root of a monic polynomial $f \in \mathbb{Z}[X]$. Then either z is an integer or z is an irrational.

This proposition can be equivalently stated as the following slogan.

Slogan. Every rational root of a monic polynomial $f \in \mathbb{Z}[X]$ is an integer.

Proof.

Idea of the proof: Suppose $z \in \mathbb{C}$ is a rational root to a monic polynomial $f \in \mathbb{Z}[X]$, then show that it is actually an integer. If it is not rational, it must be irrational so this part takes care of itself.

Let $f \in \mathbb{Z}[X]$ be monic with $f(X) = X^m + c_{m-1}X^{m-1} + \ldots + c_1 X + c_0$. Suppose $a/b \in \mathbb{Q}$ is a root of $f(X)$. WLOG, assume $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and $\gcd(a, b) = 1$. Then,

$$0 = f(a/b) = (a/b)^m + c_{m-1}(a/b)^{m-1} + \ldots + c_1(a/b) + c_0$$

Multiply both sides by b^m to have

$$0 = a^m + \underbrace{c_{m-1}a^{m-1}b + \ldots + c_1 ab^{m-1} + c_0 b^m}_{b \text{ divides this}}$$

So, rearranging we have

$$a^m = -bk$$

for some $k \in \mathbb{Z}$ i.e. b divides a^m. But, we assumed $\gcd(a, b) = 1$, so the only way this is possible is if $b = 1$.

Thus, if $a/b \in \mathbb{Q}$ is a root of $f(X)$, $a/b = a \in \mathbb{Z}$. ∎

Remark. We need **MONIC**. Repeat with me, we **NEED MONIC**. Consider $2X - 1$, then $x = 1/2$ is a rational root which is not an integer.

Example. Some applications of the theorem.

1. $\sqrt{2}$ is a root of $X^2 - 2$. By the proposition above, $\sqrt{2}$ is an integer or irrational. But, 2 is not a square of any integer. So, $\sqrt{2}$ is irrational.

2. $\sqrt[3]{17}$ is a root of $X^3 - 17$. Because 17 is a prime, there does not exists an integer that squares to 17, so by the proposition above, $\sqrt[3]{17}$ is irrational.

3. In fact, we can generalize and see that $\sqrt[d]{p}$ is irrational for $d \geqslant 2$ and p prime.

Theorem 9.2. (Euler, 1737). $e = \sum_{n=0}^{\infty} 1/n!$ is irrational.

This was first proven by Euler, but we will give a proof due to Fourier. Euler's proof uses continued fractions which we don't cover in this notes.

Proof. Suppose e is rational. Then, $e = a/b \in \mathbb{Q}$ where we can assume WLOG that $a \in \mathbb{Z}, b \in \mathbb{N}$ and $\gcd(a, b) = 1$. Now, consider

$$S_m = \sum_{n=1}^{m} \frac{1}{n!} \in \mathbb{Q}$$

where $S_m \to e$ as $m \to \infty$. Suppose $m \geqslant b$. Then, $m!e \in \mathbb{N}$ and $m!S_m \in \mathbb{N}$. It follows that

$$m!(e - S_m) \in \mathbb{N} \qquad (*)$$

because $e - S_m > 0$. But then,

$$\begin{aligned} m!(e - Sm) &= m!\left(\frac{1}{(m+1)!} + \frac{1}{(m+2)!} + \dots\right) \\ &= \frac{1}{m+1} + \frac{1}{(m+1)(m+2)} + \frac{1}{(m+1)(m+2)(m+3)} + \dots \\ &< \underbrace{\frac{1}{m+1} + \frac{1}{(m+1)^2} + \frac{1}{(m+1)^3} + \dots}_{\text{this is just a geometric series}} \\ &= \frac{1}{m+1}\left(\frac{1}{1 - \frac{1}{m+1}}\right) \\ &= \frac{1}{m} \end{aligned}$$

So, it follows that we have

$$0 < m!(e - S_m) < \frac{1}{m}$$

However, a number strictly between 0 and $1/m$ where $m \in \mathbb{N}$ (or even $\mathbb{Z}$) **cannot** be an integer. This contradicts $(*)$. We are done. ∎

because $b \leqslant m$, thus $b | m!$. Think about it, $3 \leqslant 5$, so $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$, thus $3|5!$. For $m!S_m$, write down terms of S_m and note that we can make the denominator $m!$. Multiplying by $m!$ thus clears the denominator, so the number must be in $\mathbb{N}$.

Theorem 9.3. (Lambert, 1761) π is irrational.

Proof. Not too hard but omitted. ∎

A natural question would then be, how about $\pi + e$, this must be irrational as well right? Well, it is an open problem — nobody knows yet. But it would be really weird for them to not be irrational.

Conjecture. $e + \pi$ is irrational.

9.2 Algebraic and Transcendental Numbers

Definition 9.2. A number $\alpha \in \mathbb{C}$ is called **algebraic** if there is a non-zero polynomial $f \in \mathbb{Q}[X]$ with $f(\alpha) = 0$. Otherwise, α is said to be **transcendental**.

of course when we said non-zero, we mean a non-constant polynomial. The only constant polynomial which have roots that make it 0 is the constant 0 function; but we assume that this should not be the case.

Example. If $a/b \in \mathbb{Q}$, then a/b is a root of the polynomial $x - a/b$, and is thus algebraic.

So, every rational number is thus algebraic. In view of the contrapositive to this statement, we have that every transcendental number is irrational.

Slogan. The slogan for this:

1. Every rational number is algebraic.
2. Every transcendental number is irrational.

Lots of irrational numbers are in fact, algebraic.

Example. $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[19]{17}$ are irrational and algebraic.

Theorem 9.4. If $\alpha, \beta \in \mathbb{C}$ are algebraic, then $\alpha + \beta$ and $\alpha\beta$ are algebraic.

Proof. Omitted. ■

Example. $\alpha = \sqrt{2}+1$ is algebraic. How to see this? Well we use the following reverse engineering trick:

"*Bring everything that is rational to one side and keep removing surds*"

$$\alpha - 1 = \sqrt{2} \implies (\alpha - 1)^2 = 2 \implies \alpha^2 - 2\alpha + 1 = 2$$

Thus,

$$\alpha^2 - 2\alpha - 1 = 0$$

So, α is a root to the polynomial $f(X) = X^2 - 2X - 1$.

Note that this method can be inefficient when done wrongly especially when you remove the first part of the trick. It would however still get you correct results.

$$\alpha = \sqrt{2} + 1 \implies \alpha^2 = (\sqrt{2} + 1)^2 = 2 + 2\sqrt{2} + 1 = 3 + \sqrt{2}$$

Then, bring everything that is rational to one side and keep removing surds.

$$\alpha^2 - 3 = \sqrt{2} \implies (\alpha^2 - 3)^2 = 4(2) \implies \alpha^4 - 6\alpha^2 + 9 = 8$$

And thus

$$\alpha^4 - 6\alpha^2 + 1 = 0$$

So, α is a root to the polynomial $g(X) = X^4 - 6X^2 + 1 = (X^2 - 2X - 1)(X^2 + 2X + 1)$.

Slogan. Bring everything that is rational to one side and keep removing surds.

For the sake of efficiency, memorize this slogan. If you want to see what more chaotic things that can happen if you don't bring the rationals to one side, do this exercise without using the slogan.

Exercise. Fun exercise. Prove that $\sqrt[3]{2} + 1$ is algebraic. In other words, find a non-zero $f \in \mathbb{Q}[X]$ such that $\sqrt[3]{2} + 1$ is a root.

Theorem 9.5. Let $\alpha \in \mathbb{C}$. If α is algebraic, then so is $1/\alpha$.

Proof. Suppose α is algebraic. Then there exist $c_i \in \mathbb{Q}$ not all zero such that

$$f(\alpha) = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} + c_n\alpha^n = 0.$$

Multiplying through by $1/\alpha^n$ we have

$$\alpha^{-n} f(\alpha) = c_0 \left(\frac{1}{\alpha}\right)^n + c_1 \left(\frac{1}{\alpha}\right)^{n-1} + \ldots + c_{n-1}\left(\frac{1}{\alpha}\right) + c_n = 0.$$

So, $g(x) = x^{-n} f(x)$ is a non-zero polynomial with rational coefficients such that $g(1/\alpha) = 0$. i.e. $1/\alpha$ is algebraic, as desired. ■

Theorem 9.6. Let $z \in \mathbb{C}$. If z is transcendental, then so is z^a for any $a \in \mathbb{Z}\backslash\{0\}$.

Note that $a \neq 0$. If $n = 0$, this is not anymore true. For example: e is transcendental but $e^0 = 1$ is not.

Proof. Fix $a \in \mathbb{Z}\backslash\{0\}$ and suppose z^a is algebraic. Then z^a is a root of some non-zero polynomial with **rational** coefficients $f(x)$. WLOG, we may assume $\deg(f) = n$ for some $n > 1$. Now if $a > 0$, then z is a root of the non-zero polynomial $f(x^a)$ and therefore, is algebraic. Otherwise, if $a < 0$, then z is a root of the non-zero polynomial $g(x) = x^{-an} f(x^a)$ and therefore is also algebraic. ■

Remark. Let's give a more explicit proof. Suppose z^a is algebraic. Then there are constants $c_i \in \mathbb{Q}$ not all zero such that

$$f(z^a) = c_0 + c_1(z^a) + \ldots c_n(z^a)^n = 0$$

So z being a root of $f(x^a)$ is clear when $a > 0$. Now suppose $a < 0$. Then write $a = -b$ for some $b > 0$. We have that

$$f(z^a) = f(z^{-b}) = c_0 + \frac{c_1}{z^b} + \ldots + \frac{c_n}{(z^b)^n} = 0$$

Multiplying by z^{-an} we have

$$z^{-an} f(z^a) = z^{bn} f(z^{-b}) = c_0(z^b)^n + c_1(z^b)^{n-1} + \ldots + c_n = 0$$

Thus, we have that z is a root of the polynomial $g(x) = x^{-an} f(x^a)$

Remark. Of course all this statement are actually *if and only if* statements! The converse is a truth due to product of algebraic numbers being algebraic. That is, if α is algebraic then so is α^n. Taking the contrapositive, if α^n is transcendental then α is transcendental.

We have an even better result.

Corollary 9.1. Let $z \in \mathbb{C}$. If z is transcendental, then so is z^q for any $q \in \mathbb{Q}\backslash\{0\}$.

Proof. Suppose z is transcendental but $y = z^q$ is algebraic for any $q \in \mathbb{Q}\backslash\{0\}$. Now write $q = a/b$ for some $a \in \mathbb{Z}\backslash\{0\}$ and $b \in \mathbb{N}$. Then $y = z^{a/b}$ and hence $y^b = z^a$. Since the product of algebraic numbers is algebraic, y^b is algebraic by hypothesis. Therefore z^a is necessarily algebraic. However, the preceding theorem tells us that z^a is transcendental for any $a \in \mathbb{Z}\backslash\{0\}$ [↯]. ■

By running the same argument as in the preceding theorem, we can conclude that if z is transcendental, then any linear combination (with rational coefficients) of powers of z is also transcendental.

Theorem 9.7. Let $z \in \mathbb{C}$. If z is transcendental, then so is $f(z)$ for any **non-constant** polynomial $f \in \mathbb{Q}[X]$.

not that non-constant and not non-zero!

Proof. We will prove the contrapositive. Let $f \in \mathbb{Q}[X]$ be a non-constant polynomial and $f(z)$ be algebraic. Then by definition of algebraicity, there is a non-zero polynomial $g \in \mathbb{Q}[X]$ such that $g(f(z)) = 0$. But then $g \circ f$ is a non-zero polynomial with rational coefficients and z is a root of it. Thus, z must be algebraic. ■

again, a non-zero polynomial with roots making it 0 is of course non-constant — cf. margin notes for definition of algebraicity.

Recall that a set X is uncountable or is an uncountably infinite set if there is no injection from X to $\mathbb{N}$. If it is countable, then there is an injection from X to $\mathbb{N}$.

Fact. There are uncountably many transcendental numbers.

You just have to believe what we will be saying for the next few lines or so (unless you want to try to prove it, then good luck!). There is a bijection between the algebraic numbers and $\mathbb{N}$. In, other words, there are countably many algebraic numbers (still infinite though). Then, transcendental numbers are just everything else but still within $\mathbb{C}$ (i.e. $\mathbb{C}$ minus algebraic numbers). We know $\mathbb{C}$ is uncountably infinite i.e. there is no bijection between $\mathbb{C}$ and $\mathbb{N}$. It follows that there are uncountably infinite transcendental numbers. Ironically, it's super hard to find them. They are like the dark matter of numbers. We know there are infinitely many of them but to exactly find them, it's just hard and tricky.

Fact. π and e are transcendental

The proof of this fact is not easy so will be omitted. So, what are the transcendental numbers that we know of? We know that this number

$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

which popped up in a previous example is transcendental. But how do we prove this? Our current machinery is not enough, we need to build more tools.

10 Diophantine Approximation

10.1 Approximating the reals using the rationals - a motivation

We are diving into the world of the real numbers, with only the rationals at our dispense. What better way there is than to understand how to approximate these reals using the rationals. We will use some analysis in here, so I hope you're ready.

From Real Analysis, we know that $\mathbb{Q} \subseteq \mathbb{R}$ is dense i.e. every real number is the limit of a convergent sequence of the rational numbers. For example,

$$e = \lim_{k\to\infty} \sum_{k=0}^{n} \frac{1}{k!}$$

In the ε-N language, we write this as for every $\varepsilon > 0$ there exists an N_ε such that whenever $n \geqslant N_\varepsilon$,

$$\left| e - \sum_{k=0}^{n} \frac{1}{k!} \right| < \varepsilon$$

Now the sequence of partial sums $\sum_{k=0}^{n} 1/(k!)$ are of course rational numbers. So, we can view of this sequence converging to e as being a rational number approximating e. Looking at the ε-N version, we can see that this approximation gets better as n gets larger i.e. the difference between e and $\sum_{k=0}^{n} \frac{1}{k!}$ gets smaller as n gets very large.

Instead of e, let's consider an arbitrary real number $\alpha \in \mathbb{R}$ such that $0 < \alpha < 1$. So, we can write its decimal expansion

$$\alpha = 0.a_1a_2a_3\ldots$$

where a_i is completely arbitrary, i.e. $0 \leqslant a_i \leqslant 9$ for all i. Now, let's find a sequence of rational numbers converging to α. Well, that's not too hard, we can just truncate the decimal expansion of α up to a certain point and this is a rational number. Suppose we truncate it up to the n-th place after the decimal point[24]. Let this sequence be defined as follows:

$$s_n = 0.a_1a_2\ldots a_n$$

or in a more compact notation, $s_n = a/10^n$ for some integer $0 \leqslant a < 10^n$ (a here is arbitrary as α is arbitrary, you have to write down some numbers for this to make sense.). Now, let us check how good of an approximation this sequence of rational numbers is to α.

$$\left|\alpha - \frac{a}{10^n}\right| = |\alpha - s_n| = |0.00\ldots0a_{n+1}a_{n+2}\ldots| < \frac{1}{10^n}$$

When we talk about how good an approximation of a real number by a rational number, we should think about the size of the denominator of the rational number approximating the real number. If we let the denominator get very-very big, then of course we can approximate the real number arbitrarily closely. This idea is embedded in the very definition of the ε-N definition of convergence (whenever the limit tends to a rational number).

In the case of our α and s_n, of course as n gets large, then obviously $s_n \to \alpha$ as we defined s_n to be the truncation of α. So, s_n is a very nice approximation to α. But, think about s_n in its compact notation. As n gets very big, the denominator of s_n which is 10^n also gets very-very large — **this suggests that there is a direct correspondence of a rational number being able to approximate the real number nicely and its**

but a_i is not all 0 or all 9 for all i as we assumed $0 < \alpha < 1$.

[24] *or rather the* 10^n*-th place. Recall that the first digit after the decimal point is said to be the tenths place and the second digit is said to be the hundredths place i.e. the* 10^2*-th place*

Compute $10^n|\alpha - s_n|$ to see that it is indeed < 1.

denominator getting very-very big. This is what we meant by *think about the size of the denominator of the approximating rational number.*

Let's look at the bigger picture and see what we've done so far. We took α and approximate it by some rational number $a/10^n$ which is just its truncation. Then, we see that this approximation is about

$$\left|\alpha - \frac{a}{10^n}\right| < \frac{1}{10^n}$$

If we let $b = 10^n$. We've shown that we can approximate α by rational numbers a/b with

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b}$$

Of course this is just a relabelling, but we will generalize this idea now. If we fix a denominator $b \in \mathbb{N}$, and try to make

$$\left|\alpha - \frac{a}{b}\right|$$

as small as possible, then, we are actually trying to make

$$|b\alpha - a|$$

if $|\alpha - a/b| = \delta$, then $|b\alpha - a| = b\delta$. So if we can make $b\delta$ small, we can make δ small.

as small as possible. We have $b\alpha \in \mathbb{R}$ and $a \in \mathbb{Z}$. We are now approximating this real number by an integer instead of a rational. Although the approximation is worse, we have better control over this difference (at least if you think about it naively).

Why did I say we have better control? Well, because it is easy to make this difference small in an intuitive way — we just need to find the closest integer a such that the difference is small. The obvious way to do it? Choose a to be the closest integer to $b\alpha$. If we do it this way, then we have

$$|b\alpha - a| \leqslant \frac{1}{2}$$

Now multiplying both sides by b we have

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2b}$$

think about it on the number line. Fix two of your favorite consecutive integers, I'll choose 2 and 3. Now imagine a number x between 2 and 3. What is the maximal distance between this number and 2 if it's closer to 2 than 3? Well it should be 1/2. It could be less. But, if it is more, then it's closer to 3 than 2 now.

So, our naive method gives us an upper bound of $1/2b$. Can we do better? Is it possible that if we choose our denominator carefully, we can always approximate the real number by a rational number which has this particular denominator? Dirichlet's Approximation Theorem tells us that we can.

TLDR. We were asking how well can we approximate a real number α by a rational number a/b. Since $\mathbb{Q}$ is dense on $\mathbb{R}$, we can approximate it quite nicely i.e. we can always make the difference between α and a/b as small as we want. However, there is a trade-off. As we force a/b to be closer and closer to α, we may have to use larger[25] and larger a and b. Whereas, a nice approximation of a/b to α means getting very much close to α, with b being relatively small. This problem leads us to the question:

"*How nice can we approximate α by a/b with the denominator not being too big?*"

[25] *try approximating $\sqrt{2}$ using a rational number. $|\sqrt{2} - 14/10| \approx 0.014214$, but $|\sqrt{2} - 14142/10^4| \approx 1.4 \times 10^5$. The latter is a better approximation but the numerator and denominator is relatively large compared to the former.*

TLDR II. Another way of thinking about a motivation for this problem is this. Suppose $\alpha \in \mathbb{R}$ such that $0 \leqslant \alpha \leqslant 1$. Can I find a rational approximation for α using a rational number of which its denominator is below a certain limit? Let's see a concrete example. Suppose $\alpha = 1/\pi = 0.31831....$ An obvious rational approximation to this number

is truncation of α to the n-th place after the decimal point, this involves powers of 10. We have $3/10, 31/100, 318/1000, 3183/10000$, and so on. But now, suppose we impose an extra condition, we only want the denominator to be as large as 10. Could we do better than $3/10$? Well, $3/9 = 0.333...$ is better. Let's loosen this condition a bit and say we want the denominator to be as large as 100. Could we do better now? Well, our best option would then be $31/97 = 0.319588...$ and this is much better than just $31/100 = 0.31$. We have been brute forcing by hand really and if we are to check the case when the decimal gets to like 10^100, this would be a mess. This leads us to the next question, can we always do better than the truncation approximation? That is, can we always find a number which has a smaller denominator than our truncation that can still approximate this number nicely?

10.2 Approximation Theorems of Dirichlet and Liouville

Theorem 10.1. (Dirichlet's Approximation Theorem). Let $\alpha \in \mathbb{R}$ and $n \in \mathbb{N}$. Then, there exists $a/b \in \mathbb{Q}$ with $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $b \leqslant n$ such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{bn}$$

Remark. Since $b \leqslant n$, we have $b^2 \leqslant bn$ and so

$$\frac{1}{bn} \leqslant \frac{1}{b^2}$$

Dirichlet's Approximation Theorem, which we will call **DAT** from now on, is an existence theorem. It answers all the questions before and says that: yes, we can always approximate any real number using rational numbers whose denominator is not too large.

Example. Take $\alpha = \sqrt{2}$ and $n = 3$. We want to make $|\alpha - a/b|$ small for $b \leqslant n = 3$. Just like before, this is the same as making $|b\alpha - a|$ small. So, we want to choose b that make this difference small for some integer a. Since $b \leqslant 3$, there are not so many choices. b can either be $1, 2$ or 3 (remember $b \in \mathbb{N}$). So, $b\alpha$ can be $1\alpha, 2\alpha$ or 3α and we have

$$1\alpha = 1.414...$$
$$2\alpha = 2.828...$$
$$3\alpha = 4.243...$$

Which one is closest to being an integer? Well, 2α is the closest, and it is close to 3 i.e. we have $|2\alpha - 3|$ is smallest amongst all $|b\alpha - a|$ for $1 \leqslant b \leqslant 3$, $a \in \mathbb{Z}$. So the best rational approximation to $\sqrt{2}$ with denominator at most 3 is $3/2$. This is how you do it directly.

If we used DAT directly, we know that we can find $a/b \in \mathbb{Q}$ with $b \leqslant 3$ such that $|\alpha - a/b| < 1/3b$.

This example is crucial in the sense that it will give the reader a direction of the proof of DAT. Let's prove it now.

Proof. (Proof of DAT). Consider the real numbers

$$0\alpha, 1\alpha, 2\alpha, \ldots, n\alpha$$

Now, take the fractional part[26] of these numbers. We have

$$\{0\alpha\}, \{1\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$$

This is a list of $n+1$ real numbers in $[0,1)$. Now, suppose we divide $[0,1)$ into n disjoint intervals of length $1/n$:

$$\left[0, \frac{1}{n}\right), \left[\frac{1}{n}, \frac{2}{n}\right), \ldots, \left[\frac{n-1}{n}, 1\right)$$

We have $n+1$ numbers in $[0,1)$, and we have n intervals whose union is $[0,1)$. The pigeonhole principle tells us that there exists $0 \leqslant i < j \leqslant n$ such that $\{i\alpha\}$ and $\{j\alpha\}$ are in the same interval (of length $1/n$). So, this implies that

$$|\{i\alpha\} - \{j\alpha\}| < \frac{1}{n} \qquad (*)$$

Now, recall that we have

$$i\alpha = \lfloor i\alpha \rfloor + \{i\alpha\} \text{ and } j\alpha = \lfloor j\alpha \rfloor + \{j\alpha\}$$

So, we have

$$(j-i)\alpha = j\alpha - i\alpha = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor + \{j\alpha\} - \{i\alpha\}$$

Rearrange to have

$$\{j\alpha\} - \{i\alpha\} = (j-i)\alpha - (\lfloor j\alpha \rfloor + \lfloor i\alpha \rfloor)$$

Replace this into $(*)$ to have

$$|(j-i)\alpha - (\lfloor j\alpha \rfloor + \lfloor i\alpha \rfloor)| < \frac{1}{n}$$

which implies

$$\left|\alpha - \frac{(\lfloor j\alpha \rfloor + \lfloor i\alpha \rfloor)}{j-i}\right| < \frac{1}{n(j-i)}$$

So, we can take $a = \lfloor j\alpha \rfloor + \lfloor i\alpha \rfloor$ and $b = j - i$, we are done. ■

[26] *the fractional part of a real number x, written as $\{x\}$, is the removal of the integer part of x. Thus, $\{x\} = x - \lfloor x \rfloor$. If x is positive, this precisely means to take every decimal digit after the decimal point. Note that $\{\cdot\} : \mathbb{R} \to [0,1)$. For x negative, we will still take the definition as $x - \lfloor x \rfloor$. It will not harm the proof as the range of $\{\cdot\}$ is still $[0,1)$.*

note that we have a **strict** inequality because the fractional parts $\{i\alpha\}, \{j\alpha\}$ are in the same interval (of length $1/n$) which are **half-open half-closed** by our choice when dividing $[0,1)$ into n *strips*. If the intervals are fully closed like $[1/n, 2/n]$, then a non-strict inequality is possible.

Corollary 10.1. Let $\alpha \in \mathbb{R}$ be **irrational**. Then, there exists infinitely many (distinct) rational numbers a/b such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$$

Remark. Equivalently, we could have write the corollary like this. Let $\alpha \in \mathbb{R}$ be irrational. Then, there exists an infinite sequence of rational numbers $a_n/b_n \to \alpha$ with

$$\left|\alpha - \frac{a_n}{b_n}\right| < \frac{1}{b_n^2}$$

if α is rational, then the sequence a_n/b_n will just tend to α itself. So, this is really vacuously true — of course it can be a finite sequence now. But it can also be an infinite sequence, just take the constant sequence $\{\alpha, \alpha, \alpha, \alpha, \ldots\}$.

Proof. Fix an $n \in \mathbb{N}$ and apply DAT. This will give us a rational number a_n/b_n with

$$\left|\alpha - \frac{a_n}{b_n}\right| < \frac{1}{nb_n} < \frac{1}{b_n^2}$$

Since $n \in \mathbb{N}$ is arbitrary, this is true for all n. ■

This corollary is what we meant by real numbers can be approximated well by rational

numbers. The approximation of α by the sequence a_n/b_n is a bit better than our initial naive way of approximating α which lead us to having the bound of $1/2b$. The slogan for DAT is thus:

Slogan. Real numbers can be approximated **well** by rational numbers.

So, we can find $a_n/b_n \to \sqrt{2}$ with

$$\left|\sqrt{2} - \frac{a_n}{b_n}\right| < \frac{1}{b_n^2}$$

Now a natural question is to ask, is there anything special about the square in b_n^2. How about b_n^3? Can we still do it? Can we find $a_n/b_n \to \sqrt{2}$ with

$$\left|\sqrt{2} - \frac{a_n}{b_n}\right| < \frac{1}{b_n^3} \ ?$$

Unfortunately, Liouville tells us we can't.

Theorem 10.2. (Liouville Approximation Theorem). Let $\alpha \in \mathbb{R}$ be an irrational algebraic number. Suppose α is a root of $f \in \mathbb{Q}[X]$ with degree $d > 0$. Then, there is a constant $C(\alpha) > 0$ such that for all $a \in \mathbb{Z}, b \in \mathbb{N}$, we have

$$\left|\alpha - \frac{a}{b}\right| > \frac{C(\alpha)}{b^d}$$

Proof. The proof of this theorem is omitted and is non-examinable. ∎

Remark. Note that $C(\alpha)$ is dependent on α. Moreover, observe very carefully how the degree of $f \in \mathbb{Q}[X]$ plays a role in the result (its degree).

Corollary 10.2. Let $\alpha \in \mathbb{R}$ be an irrational algebraic number. Suppose α is a root of $f \in \mathbb{Q}[X]$ with degree $d > 0$. Moreover, suppose we are given $\varepsilon > 0$. Then the inequality

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{b^{d+\varepsilon}}$$

holds for only finitely many $a \in \mathbb{Z}, b \in \mathbb{N}$.

Remark. The ε is completely arbitrary. It is given, so you can take it to be as large or as small as you want.

Slogan. Algebraic irrational numbers cannot be approximated **very well** by rational numbers.

Proof. Let α be an irrational algebraic number which is a root of $f \in \mathbb{Q}[X]$ with degree m. By Liouville's Theorem, there exists $C(\alpha) > 0$ such that

$$\left|\alpha - \frac{a}{b}\right| > \frac{C(\alpha)}{b^m} \qquad (*)$$

Now, suppose we have $a \in \mathbb{Z}, b \in \mathbb{N}$ such that

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{b^{m+\varepsilon}} \qquad (\dagger)$$

Combining $(*)$ and $(\dagger)$ we have that

$$\frac{C(\alpha)}{b^m} \leqslant \frac{1}{b^{m+\varepsilon}}$$

This implies that

$$b^{\varepsilon} < \frac{1}{C} \implies b < \frac{1}{C^{1/\varepsilon}}$$

This says that there are only finitely many possibilities for b. Moreover, by $(\dagger)$, for each fixed b, there are only finitely many possibilities for a. Together, there are only finitely many possibilities of a and b. ■

Remark. Liouville's Theorem implies the Corollary but the other way around, despite to be seemingly true, is **NOT** true! Consider the function $\frac{1}{b^d \log b}$. This number satisfies the inequality

$$\frac{1}{b^d \log b} \leqslant \frac{1}{b^{d+\varepsilon}}$$

for only finitely many positive integers b. However, there does not exist any real number $C > 0$ such that

$$\frac{1}{b^d \log b} > \frac{C}{b^d}$$

for all positive integers b.

Example. Take $\alpha = \sqrt{2}$. This is an algebraic irrational number as it is a root of $f(X) = X^2 - 2$ where $\deg(f) = m = 2$. We can take ε to be as small as we want. Suppose $\varepsilon = 1$. Then, by the corollary to Liouville's theorem, there are only finitely many rational numbers a/b with

$$\left|\sqrt{2} - \frac{a}{b}\right| \leqslant \frac{1}{b^3}$$

Exercise. Convince yourself that there are indeed only finitely many $a/b \in \mathbb{Q}$ such that the above inequality holds.

Remember that before we make the transition into this subsection, we wanted to prove a certain number is transcendental but didn't have sufficient tools? Now we do.

Corollary 10.3. The number $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.

Proof. Suppose $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is algebraic such that it is a root of a degree $d > 0$ polynomial with rational coefficients. By Liouville, there is a $C(\alpha) > 0$ such that for every $a \in \mathbb{Z}, b \in \mathbb{N}$,

$$\left|\alpha - \frac{a}{b}\right| > \frac{C(\alpha)}{b^d} \qquad (*)$$

Now, consider $s_N = \sum_{n=1}^{N} \frac{1}{10^{n!}} = A/B$ which is a rational number with $B = 10^{N!}$

and A some integer. Then,

$$\begin{aligned}
\left|\alpha - \frac{A}{B}\right| &= \sum_{n=N+1}^{\infty} \frac{1}{10^{n!}} \\
&= \frac{1}{10^{(N+1)!}} + \frac{1}{10^{(N+2)!}} + \frac{1}{10^{(N+3)!}} + \dots \\
&= \frac{1}{10^{(N+1)!}} \left(1 + \frac{1}{10^{(N+2)!-(N+1)!}} + \frac{1}{10^{(N+3)!-(N+1)!}} + \dots\right) \\
&< \frac{1}{10^{(N+1)!}} \underbrace{\left(1 + \frac{1}{10^1} + \frac{1}{10^2} + \dots\right)}_{\text{geometric series}} \\
&= \frac{1}{10^{(N+1)!}} \frac{1}{1 - 1/10} \\
&< \frac{2}{10^{(N+1)!}} \qquad (\dagger)
\end{aligned}$$

Thus, combining $(\dagger)$ and $(*)$ we have

$$\frac{C(\alpha)}{10^{N!d}} = \frac{C(\alpha)}{B^d} < \left|\alpha - \frac{A}{B}\right| < \frac{2}{10^{(N+1)!}}$$

This implies that

$$10^{(N+1)!-N!d} < \frac{2}{C(\alpha)}$$

and this is true for all $N \in \mathbb{N}$. But then, the LHS $\to \infty$ as $N \to \infty$. This contradicts the fact that it is bounded by $2/C(\alpha)$. So, α cannot be algebraic. ■

PART

IV

Diophantine Equations

Definition 10.1. (Diophantine Equation). A **Diophantine equation** is a polynomial equation with integer coefficients

$$f(X_1, \ldots, X_r) = 0$$

where we seek only integer solutions.

Given a Diophantine equation, it is only natural to ask how many solutions (if there are any) does this equation have and even more so, if there is any algorithm to find a general solution. Unfortunately, the latter question has a negative answer — that is, such a general solution does not exist (cf. Hilbert's tenth problem). We've met the simplest case of Diophantine equations before, which is a linear Diophantine equation

$$aX + bY = c$$

We know when solutions to this equation exists — when $\gcd(a, b)$ divides c. We know there are $\gcd(a, b)$ solutions. We even know a form of the general solution to this equation. In fact, we can generalise this quite easily.

Theorem 10.3. Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ not all zero. Let $c \in \mathbb{Z}$. Then, the linear equation

$$a_1X_1 + \ldots + a_nX_n = c$$

has a solution in $\mathbb{Z}$ if and only if $\gcd(a_1, \ldots, a_n)|c$.

Proof. Exercise. ∎

We are basically done with linear Diophantine equations. Let's look at quadratic Diophantine equations now, the simplest case being the Pythagorean equation.

11 Pythagorean Triples

Our aim in this section is to try to describe all the integer solutions (x, y, z) to the equation $x^2 + y^2 = z^2$.

Definition 11.1. A **Pythagorean triple** is a set of three positive integers (x, y, z) such that $x^2 + y^2 = z^2$. We say that the triple is **primitive** if $\gcd(x, y, z) = 1$.

A right-angled triangle whose side lengths are integers is called a **Pythagorean triangle**. Moreover, its side lengths form a Pythagorean triple. From now on, we may just call a Pythagorean triple as a **triple**.

If we have a triple (x, y, z), we can get infinitely many other triples through scaling (x, y, z) by a factor $\lambda \in \mathbb{N}$. This is true because

$$(\lambda x)^2 + (\lambda y)^2 = \lambda^2 x^2 + \lambda^2 y^2 = \lambda^2(x^2 + y^2) = \lambda^2 z^2 = (\lambda z)^2$$

So, $(\lambda x, \lambda y, \lambda z)$ is another triple.

Example. $(3, 4, 5)$ and $(5, 12, 13)$ are primitive triples. $(6, 8, 10)$ is a non-primitive triple.

Notice that $2 = \gcd(6, 8, 10)$. And that $(6/2, 8/2, 10/2) = (3, 4, 5)$ is primitive. In general, if we have (x, y, z) to be a Pythagorean triple and $d = \gcd(x, y, z)$, then

$$\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$$

is a **primitive** triple. This suggests that we can produce all Pythagorean triples by taking primitive triples (x, y, z) and considering (dx, dy, dz) for some $d \in \mathbb{N}$. The conclusion is thus, **to describe all Pythagorean triples, it is enough to describe primitive Pythagorean triples**.

Lemma 11.1. Suppose (x, y, z) is a primitive Pythagorean triple. Then, any two of x, y and z are coprime.

We could reformulate this lemma to say that suppose (x, y, z) is a triple such that $\gcd(x, y, z) = 1$. Then, $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.

Remark. Note that we need it to be a **primitive Pythagorean triple** for the lemma to work. Being primitive alone is not sufficient. Take $(2, 3, 4)$, this is primitive $(\gcd(2, 3, 4) = 1)$ but not a Pythagorean triple. It is then clear that $\gcd(2, 4) \neq 1$ so the lemma fails.

Proof. Since (x, y, z) is a triple, $z^2 = x^2 + y^2$. Now, suppose d is a positive common divisor of x and y. This implies that $d^2 | z^2$ so $d | z$. But, (x, y, z) is primitive. Since d divides x, y and z, it follows that $d = 1$. Thus, x and y are coprime. Same argument works to show that $\gcd(y, z) = \gcd(x, z) = 1$, just rearrange $z^2 = x^2 + y^2$ to be $x^2 = z^2 - y^2$ and $y^2 = z^2 - x^2$ respectively. ∎

We will give a lemma for which is seemingly obvious, but will help in the proof of the upcoming proposition.

Lemma 11.2. Let $x \in \mathbb{Z}$. Then,

(1). x is even $\iff x^2 \equiv 0 \pmod 4$

(2). x is odd $\iff x^2 \equiv 1 \pmod 4$

Proof. We prove them separately.

(1). x is even $\iff x = 2k \iff x^2 = 4k^2 \equiv 0 \pmod 4$.

(2). x is odd $\iff x = 2k+1 \iff x^2 = (2k+1)^2 = 4(k^2+k)+1 \equiv 1 \pmod 4$.

■

Now, let's think about the parity[27] of x, y, z where (x, y, z) is a primitive triple. Now, Lemma (11.1) tells us that any two of x, y, z are coprime. Therefore, at **most one** of x, y, z **is even**. Now, let's go back to the equation $x^2 + y^2 = z^2$ and think about whether it is possible that none of them are even i.e. all of x, y, z is odd. This is impossible because odd + odd = even. This means that we can't have all of x, y, z odd either. Thus, we conclude that **exactly one** of x, y, z **is even**.

[27] *being even or odd*

Proposition 11.1. Suppose (x, y, z) is a primitive Pythagorean triple. Then, z is odd, one of x, y is even and the other is odd.

Proof. Suppose (x, y, z) is a primitive Pythagorean triple. Now, exactly one of x, y, z is even. Suppose z is even, so x, y are odd. By Lemma (11.2), $x^2 \equiv y^2 \equiv 1 \pmod 4$. So,

$$z^2 \equiv x^2 + y^2 \equiv 2 \pmod 4$$

This is a contradiction to Lemma (11.2) as square of even numbers are 0 mod 4.

Thus, exactly one of x and y is even. ■

Now, we have reduce our problem even more. To describe all the primitive Pythagorean triples, it is now enough to describe primitive triples (x, y, z) with x even. We can just swap x and y to get the rest of the triples. For example, $(4, 3, 5)$ is a triple. Swapping 4 and 3 gives you another triple $(3, 4, 5)$.

Remark. From now on, we will assume that x is the one that is even in the triple (x, y, z), and y is odd.

This is a useful trick that we will use and abuse.

Lemma 11.3. Suppose $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$ such that $ab = c^2$ for some $c \in \mathbb{Z}$. Then, a and b are themselves square.

Proof. Consider prime factorisations. Since ab is a square, all the powers in the prime factorisation of ab are even. But since a and b are coprime, all the powers in the prime factorisation of a and b respectively are even. Thus, a and b are square themselves. ■

We are ready to prove the grand theorem of this section.

Theorem 11.4. (Classification Theorem). Let (x, y, z) be primitive Pythagorean triples with x even. Then, there exist $s > t > 0$ such that $s \not\equiv t \pmod 2$ and

$\gcd(s,t)=1$ with

$$x=2st,\quad y=s^2-t^2,\quad z=s^2+t^2$$

Conversely, given $s>t>0$ such that $s\not\equiv t \pmod 2$ and $\gcd(s,t)=1$, then $(2st, s^2-t^2, s^2+t^2)$ is a primitive Pythagorean triple.

Remark. Few remarks.

1. s,t do not have to satisfy any equations. They're just any integers with the properties that we impose on them.
2. $s\not\equiv t \pmod 2$ is a fancy way of saying that either s or t is even and the other is odd.
3. Why do we need $s>t$? So that, $s^2>t^2$ i.e. so that $y\in\mathbb{N}$
4. Why do we need $s\not\equiv t \pmod 2$? Because if $s\equiv t \pmod 2$, then all x,y,z will be even. Thus, (x,y,z) won't be primitive.
5. Why do we need $\gcd(s,t)=1$? Because if $d|s$ and $d|t$, then d divides[28] x,y and z. Thus, (x,y,z) won't be primitive.

[28] *we assumed (x,y,z) is primitive remember. So it doesn't make sense if $y=s^2-t^2$ and $z=s^2+t^2$ but $\gcd(s,t)\neq 1$ as $\gcd(s,t)$ divides both y and z. If any positive integer dividing both y and z, it better be 1*

Let's prove the theorem now.

Proof. ($\Longleftarrow$). Let $s>t>0$ integers such that $s\not\equiv t \pmod 2$ and $\gcd(s,t)=1$. Assume for contradiction that $(2st, s^2-t^2, s^2+t^2)$ is not a primitive Pythagorean triple. So, suppose we have a prime p such that $p|(s^2-t^2)$ and $p|(s^2+t^2)$. Then,

$$p|(s^2-t^2)+(s^2+t^2)=2s^2$$

and

$$p|(s^2-t^2)-(s^2+t^2)=2t^2$$

Case I: $p=2$. Suppose $p=2$. Then, $2|s^2-t^2$. But we assumed $s\not\equiv t \pmod 2$. So, s^2-t^2 must be odd. [↯]

Case II: $p>2$. Suppose $p>2$. Then, by Euclid's Lemma,

$$p|2s^2 \implies p|s^2 \implies p|s$$

Similarly, $p|t$ because $p|2t^2$. But $\gcd(s,t)=1$, so p must be 1. [↯]

($\Longrightarrow$). Let (x,y,z) be a primitive Pythagorean triple with x even. Since y,z odd, there exist $u,v\in\mathbb{Z}$ such that $z-y=2u$ and $z+y=2v$. So, we can rewrite $x^2+y^2=z^2$ as

$$x^2=z^2-y^2=(z-y)(z+y)=4uv$$

that is we have $(x/2)^2=uv$.

Now, **I claim that $\gcd(u,v)=1$.** Why is this claim useful? If u and v are coprime and uv is a square, then by Lemma (11.3), u and v are themselves square. Let's prove this claim. Suppose $d>0$ divides u and v, then d divides $v+u=z$ and $v-u=y$. Since y and z are coprime, we are forced to have $d=1$. Since $d|\gcd(u,v)$, we must have that $\gcd(u,v)=1$.

$2v+2u=2z$ and $2v-2u=2y$. Dividing by 2 on both equations explains our implication.

We can apply Lemma (11.3) now. By that lemma, u and v are square themselves.

Let $u = t^2$ and $v = s^2$ with $s, t > 0$. By definition of a Pythagorean triple (not necessarily primitive), we require $y > 0$, so we must have $v > u$ i.e. $s > t > 0$. Now, we can rewrite $x^2 + y^2 = z^2$ as

$$x^2 = z^2 - y^2 = (z - y)(z + y) = 4uv = 4(st)^2$$

So, $x = 2st$. Moreover because $v + u = z$ and $v - u = y$, altogether we have:

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2 + t^2$$

Since $\gcd(y, z) = 1$, we have[29] that $\gcd(s, t) = 1$. Moreover, because y is odd, we can't have $s \equiv t \pmod 2$ otherwise then $y \equiv 0 \pmod 2$ i.e. y is even, so $s \not\equiv 2 \pmod 2$. ■

[29] *Suppose* $\gcd(s, t) \neq 1$, *then let* p *be a prime dividing* s *and* t. *Thus,* $p|s^2$ *and* $p|t^2$. *This implies* p *divides* $s^2 + t^2 = z$ *and* $s^2 - t^2 = y$ *[↯]*

Remark. Note that the Classification Theorem implies that if (x, y, z) is a primitive Pythagorean triple, then we can get all Pythagorean triples (up to swapping x and y) by taking s and t that satisfies the theorem with another positive integer $d > 0$ and consider

$$x = 2dst, \quad y = d(s^2 - t^2), \quad z = d(s^2 + t^2)$$

Let's discuss some example applications. Let's think about primitive Pythagorean triples with an extra condition.

Example. Find all primitive Pythagorean triples (a, b, c) with $c = b + 3$. Note that the hypotenuse is always odd i.e. c is odd. So, $b = c - 3$ is even. Therefore, a is odd. Suppose (a, b, c) is a primitive Pythagorean triple. By the Classification Theorem, there exist $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$ with $b = 2st$, $a = s^2 - t^2$ and $c = s^2 + t^2$. Now,

$$s^2 + t^2 = b + 3 = 2st + 3$$

so we have

$$s^2 - 2st + t^2 = 3 \implies (s - t)^2 = 3$$

But there are no such $s > t > 0$ that satisfies this equation. Therefore, we conclude there are no solutions.

Example. Find all primitive Pythagorean triples (a, b, c) with $c = b + 2$. Let's think parity first. Since c is always odd, we have $b = c - 2$ by the constraint so b is odd. One of a, b, c must be even, so a is even. By the Classification Theorem, there exists $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$ with $a = 2st$, $b = s^2 - t^2$ and $c = s^2 + t^2$. Now,

$$s^2 + t^2 = c = b + 2 = s^2 - t^2 + 2$$

so we have

$$2t^2 = 2 \implies t^2 = 1$$

Because $t > 0$, this implies $t = 1$. Now, let's check the conditions on s. We have $s > 1$. We have $\gcd(s, 1) = 1$ and $s \not\equiv 1 \pmod 2$ which implies that s is even. Altogether, we have that s is any positive even number. Therefore

$$(a, b, c) = (2s, s^2 - 1, s^2 + 1)$$

12 Fermat's Last Theorem

Theorem 12.1. (Wiles-Taylor, 1994). If $n \geqslant 3$, there are no positive integer solutions (x, y, z) to the equation

$$x^n + y^n = z^n$$

This theorem is known as Fermat's Last Theorem and it is super hard to proof, like super super hard. The simplest case of this theorem is when $n = 4$ (yes, not $n = 3$) and this may be the only case of which proof was known to Fermat. In fact, we will use **Fermat's method of descent** or better known as the **method of infinite descent** to prove a stronger result than this.

Theorem 12.2. There are no positive integer solutions (x, y, z) to the equation

$$x^4 + y^4 = z^2$$

Note that this implies that there are then no positive integer solutions (x, y, z) to the equation $x^4 + y^4 = z^4$ as we can write $z^4 = (z^2)^2$. Taking the contrapositive, if (a, b, c) solves $x^4 + y^4 = z^4$, then (a, b, c^2) solves $x^4 + y^4 = z^2$.

Before we start with the proof, let us give some **idea** of how we will do it. The proof will be by contradiction and it goes by the following steps.

1. We will start with a positive integer solution (a, b, c).
2. Then, we will construct a new solution (a_1, b_1, c_1) with $c_1 < c$. This is the descent step.
3. Then, we go on and construct a new solution (a_2, b_2, c_2) with $c_2 < c_1$.
4. Then, we realize there's nothing stopping us to do this indefinitely. We go on and do the same thing infinitely many times, this is the so-called infinite descent step.
5. We will by now produce an infinite sequence of positive integer solutions (a, b, c), (a_1, b_1, c_1), $(a_2, b_2, c_2), \ldots$ with $c > c_1 > c_2 > \ldots$.
6. The contradiction is coming now. Since $c > c_1 > c_2 > c_3 > \ldots$ is an infinite sequence of decreasing positive integers (i.e. we can always keep going), this is impossible as it is suppose to collapse down to 0, so there is no such sequence. [ϟ]

Another way of thinking about this infinite descent argument is like this. Suppose we have a positive integer solution $(a_{\min}, b_{\min}, c_{\min})$ to the equation $x^4 + y^4 = z^2$. We can pick $(a_{\min}, b_{\min}, c_{\min})$ so that $c_{\min}$ is as small as possible (i.e. all other solutions (a, b, c) have $c \geqslant c_{\min}$). Then, we do the descent step to produce a new solution (a', b', c') with $c' < c_{\min}$ but we assumed $c_{\min}$ to be the smallest so this is a contradiction [ϟ].

Let's prove the theorem now.

Proof. Suppose (a, b, c) is a positive integer solution to $x^4 + y^4 = z^2$. This implies that (a^2, b^2, c) is a Pythagorean triple. Moreover, we can assume WLOG that (a^2, b^2, c) is a primitive Pythagorean triple. Otherwise, suppose p is a common prime divisor of a^2 and b^2. Then, $p|a$ and $p|b$. So, we have $p^2|a^2$ and $p^2|b^2$. Moreover, we also have $p^4|a^4$ and $p^4|b^4$. Therefore $p^4|(a^4 + b^4) = c^2$ i.e. we have $p^2|c$. Thus,

$$\left(\frac{a^2}{p^2}, \frac{b^2}{p^2}, \frac{c}{p^2}\right)$$

is a new smaller Pythagorean triple (**not necessarily primitive**). We can repeat this until we get a solution that is a primitive Pythagorean triple — and we can always do this. Furthermore, we can assume WLOG[30] that a^2 is even and hence, a is even. Now, by the Classification Theorem of PPT, there exist $s > t > 0$ with $\gcd(s,t) = 1$ and $s \not\equiv t \pmod 2$ such that

$$a^2 = 2st, \quad b^2 = s^2 - t^2, \quad c = s^2 + t^2 \qquad (*)$$

But observe that $b^2 = s^2 - t^2$ if and only if $s^2 = b^2 + t^2$. So, (s, b, t) is a Pythagorean triple. Notice that because a^2 is even, then b^2 is odd and hence, b must be odd. Therefore, t must be even (as we always assume the hypotenuse to be odd). Since $\gcd(s,t) = 1$, we have $\gcd(s,b,t) = 1$ so (s,b,t) is primitive. Great! We can apply the Classification Theorem again now. By the Classification Theorem there exist $u > v > 0$ with $\gcd(u,v) = 1$ and $u \not\equiv v \pmod 2$ such that

$$t = 2uv, \quad b = u^2 - v^2, \quad s = u^2 + v^2 \qquad (\dagger)$$

Now substitute $(\dagger)$ into $(*)$. Let's look what happens to a^2:

$$a^2 = 2st = 2(u^2 + v^2)(2uv) = 4uv(u^2 + v^2)$$

i.e. we have $(a/2)^2 = uv(u^2 + v^2)$. Now, because $\gcd(u,v) = 1$, I claim that $\gcd(uv, u^2 + v^2) = 1$. Proof. Suppose p is a prime dividing uv and $u^2 + v^2$. By Euclid's Lemma, $p|(uv) \implies p|u$ or $p|v$. WLOG, assume $p|u$. So, we have $u \equiv 0 \pmod p \implies u^2 \equiv 0 \pmod p$. We also have $u^2 + v^2 \equiv 0 \pmod p \implies v^2 \equiv -u^2 \equiv 0 \pmod p$. Thus, p also divides v i.e. $p|u$ and $p|v$. But, we assumed $\gcd(u,v) = 1$. [↯]. Therefore, we can apply Lemma (11.3) to say that uv and $u^2 + v^2$ are themselves square. It is even easier to see that $\gcd(u, v(u^2 + v^2)) = \gcd(v, u(u^2 + v^2)) = 1$ using the same argument as above, we leave this as an exercise. So, we can again apply Lemma (11.3) to say that u and v are also squares. Therefore, we can write

$$u = a_1^2, \quad v = b_1^2, \quad u^2 + v^2 = c_1^2$$

Plugging in u and v in terms of a_1 and b_1 respectively into the equation $u^2 + v^2 = c_1^2$, we have

$$c_1^2 = a_1^4 + b_1^4$$

It is not too difficult to see that we now have (a_1, b_1, c_1) to be a solution to the equation $x^4 + y^4 = z^2$. The punchline comes now, observe that

$$c_1^2 = u^2 + v^2 = s < s^4 + t^4 + 2(st)^2 = (s^2 + t^2)^2 = c^2$$

so $c_1 < c$. This completes the descent step. However, there's nothing stopping us from repeating this procedure indefinitely — think of starting the whole argument with (a_1, b_1, c_1) as the initial solution now. So, we can repeat this same argument to produce an infinite sequence of **positive integers** $c > c_1 > c_2 > \dots$ and this is impossible as it is suppose to terminate (in finite steps) to 0. [↯] ■

If you don't like this business of infinite descent and favour only a single descent, you can use "the solution of which $c_{\min}$ is as small as we can make it" argument. It works perfectly the same but the contradiction is more obvious to some.

[30] *otherwise, we can just swap a and b*

13 More General Diophantine Equations

We will now move to discussing general Diophantine equations. We will not be able to tame this one as we are now starting to touch very deep waters. Let's first give a recap of what is a Diophantine equation. A Diophantine equation is an algebraic equation with integer coefficients (usually with more than one unknown) which admits only integer solutions. We met with linear and quadratic Diophantine equations. How about a more general one?

Example. $x^3 - 2x = 0$. This Diophantine equation has only $x = 0$ as a solution. To see this,

$$x^3 - 2x = x(x^2 - 2) = 0 \iff x = 0 \text{ or } x^2 - 2 = 0$$

But there is no integer which satisfies $x^2 - 2 = 0$. So, we conclude that $x = 0$ is the only solution.

Example. $x^4 + 2x^2 - 4xy + 2y^2 - 1 = 0$ has solutions $x = y = 1$ and $x = y = -1$. To see this,

$$x^4 + 2x^2 - 4xy + 2y^2 - 1 = x^4 + 2(x - y)^2 - 1$$

So,

$$\begin{aligned} x^4 + 2x^2 - 4xy + 2y^2 - 1 = 0 &\iff x^4 + 2(x - y)^2 = 1 \\ &\iff x - y = 0 \text{ and } x^4 = 1 \\ &\iff x = \pm 1 \text{ and } x = y \end{aligned}$$

Example. $x^3 = 5y^6$ has solution $x = y = 0$ and nothing else. $x = y = 0$ being a solution is obvious. Now, suppose $y \neq 0$, then $x \neq 0$. Let α and β be the exponent of 5 in the prime factorisation of x and y respectively. Then

$$x^3 = 5y^6 \implies 3\alpha = 6\beta + 1 \implies 1 = 3(\alpha - 2\beta) \implies 3|1 \text{ [↯]}$$

This a contradiction, so there is no solution with $y \neq 0$.

Suppose $x = m5^\alpha$ and $y = n5^\beta$. If $x^3 = 5y^6$ for some $m, n \in \mathbb{N}$, then $m^3 5^{3\alpha} = 5n^6 5^{6\beta} \implies m^3 5^{3\alpha} = n^6 5^{6\beta+1}$. If this is true then it better be that $m^3 = n^6$ and $5^{3\alpha} = 5^{6\beta+1}$.

Theorem 13.1. If $p \equiv 3 \pmod 4$ and $p|(x^2 + y^2)$, then $p|x$ and $p|y$.

Proof. Suppose for contradiction that p does not divide x. Now, $p|(x^2 + y^2)$ so we can rewrite it as $y^2 \equiv -x^2 \pmod p$. This implies that

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

But then, $p \equiv 3 \pmod 4$ so this is impossible by the First Supplementary Law [↯]. By the same reasoning $p|y$. ∎

13.1 Congruences to the rescue

Let's look at how congruences can help us to analyse Diophantine equations. Let $f(x_1, \ldots, x_r)$ be a polynomial with integer coefficients. Now, suppose $f(x_1, \ldots, x_r) = 0$ has a solution in $\mathbb{Z}$, then it must be for sure that for every $m \in \mathbb{N}$, the congruence equation $f(x_1, \ldots, x_r) \equiv 0 \pmod m$ has a solution. Taking the contrapositive we have the following lemma.

Lemma 13.2. (Silly Lemma). If there exists an $m \in \mathbb{N}$ such that an equation has no solutions modulo m, then the equation has no solutions in integers.

Note that this is true whether m is prime or not. Let's see how this is useful by looking at examples.

Example. *The equation $x^2 = y^5 + 7$ has no solutions.*

Consider the equation modulo 11.

$$x^2 \equiv y^5 + 7 \pmod{11}$$

Let's look at each sides.

LHS. By brute force, we have that $x^2 \equiv 0, 1, 3, 4, 5, 9 \pmod{11}$.

RHS. Euler's criterion gives us $y^5 \equiv \left(\frac{y}{11}\right)$ which implies $y^5 \equiv -1, 0, 1 \pmod{11}$. Therefore, $y^5 + 7 \equiv 6, 7, 8 \pmod{11}$.

Conclusion. Since there are no overlapping solutions on the RHS and LHS, we conclude there are no solutions to $x^2 \equiv y^5 + 7 \pmod{11}$ and hence no solutions in $\mathbb{Z}$ to $x^2 = y^5 + 7$ by the Silly Lemma.

Example. *The Diophantine equation $x^{12} + y^{12} = z^{12} + w^{12} + 3$ has no solutions.*

Consider the equation modulo 13.

$$x^{12} + y^{12} \equiv z^{12} + w^{12} + 3 \pmod{13}$$

As usual, let's look at each side.

LHS. By Fermat's Little Theorem, $x^{12} \equiv y^{12} \equiv 0, 1 \pmod{13}$. So, we have

$$x^{12} + y^{12} \equiv 0, 1, 2 \pmod{13}$$

RHS. Similarly, by Fermat's Little Theorem again, $z^{12} + w^{12} \equiv 0, 1, 2 \pmod{13}$. So, we have

$$z^{12} + w^{12} + 3 \equiv 3, 4, 5 \pmod{13}$$

Conclusion. Since there are no overlapping solutions on the RHS and LHS, we conclude there are no solutions to $x^{12} + y^{12} \equiv z^{12} + w^{12} + 3 \pmod{13}$ and hence no solutions in $\mathbb{Z}$ to $x^{12} + y^{12} = z^{12} + w^{12} + 3$ by the Silly Lemma.

The following example is a bit different from the two previous examples as there are no Euler's Criterion or Fermat's Little Theorem tricks to be used.

Example. *Find all integer solutions of $15x^2 - 7y^2 = 9$.*

Suppose (x_1, y_1) is a solution. Then, $7y_1^2 = 15x_1^2 - 9 = 3(5x_1^2 - 3)$ which implies $3|(7y_1^2)$ which further implies that $3|y_1$. Now, write $y_1 = 3y_2$. Then, substituting this into the original equation gives $5x_1^2 - 21y_2^2 = 3$. Now, this implies that $3|5x_1^2$ and hence $3|x_1$. Write $x_1 = 3x_2$. Substitute into the previous equation (not original) gives $15x_2^2 - 7y_2^2 = 1$. Consider the equation modulo 3. We have

$$\text{LHS} \equiv 15x_2^2 - 7y_2^2 \equiv -1y_2^2 \pmod{3}$$

and after considering RHS we have

$$y_2^2 \equiv -1 \pmod{3}$$

This has no solutions by the First Supplementary Law as $3 \not\equiv 1 \pmod 4$. By, Silly Lemma, the equation $15x_2^2 - 7y_2^2 = 1$ has no solutions and therefore the original one does not have any solution.

In the first example we showed that the equation $x^2 = y^5 + 7$ has no solutions by using Euler's Criterion. To demonstrate why solving Diophantine equations is not a walk in the park, we'll see in the example below how tweaking the exponents a bit leads to using completely different tricks to solve it.

Example. *Find all integer solutions of* $y^2 = x^3 + 7$.

Let's check parity first. Suppose x is even, then[31] $y^2 \equiv 3 \pmod 4$ which is absurd as a square is congruent to either 0 or 1 mod 4. So, x is odd. Then, $y^2 \equiv x^3 + 7 \equiv 0 \pmod 2$, so y is even. Moreover, if $x \equiv 3 \pmod 4$, then $y^2 \equiv 3^3 + 7 \equiv 2 \pmod 4$ which again does not make sense. Therefore, $x \equiv 1 \pmod 4$. Now, let's rewrite the equation as

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$$

From here, there are plenty of ways to reach a contradiction. We will go by the easiest. Since $x \equiv 1 \pmod 4$, we have $x + 2 \equiv 3 \pmod 4$. This implies that there exists a prime $p \equiv 3 \pmod 4$ dividing the RHS. We can then take modulo p on both sides to have

$$y^2 \equiv -1 \pmod p$$

But $p \equiv 3 \pmod 4$, this contradicts the First Supplementary Law [ϟ]. Thus, the equation as no solutions in $\mathbb{Z}$.

[31] $2^j \equiv 0 \pmod 4$ *for* $j > 1$. *So whether* $x \equiv 0, 2 \pmod 4$, $x^3 \equiv 0 \pmod 4$.

Moral of this example?

Slogan. Check parities of each variables when solving Diophantine equations.

We credit Dr. Tsoi for this slogan.