Number Theory

Vinesh Ramgi

April 7, 2018

Abstract

What did the number theorist say as he drowned?

Log, log, log, log....

For an up to date version of this pdf, check my GitHub :)

https://github.com/vrvinny/number-theory

Contents

1 Introduction/Review

1.1 Introduction

Number Theory is the theory of the ring $\mathbb{Z}$ and other related rings. A ring (in this course) is a set R with two binary operations $+$ and $*$ such that:

- $(R, +)$ is an abelian group
- $*$ is associative, commutative and has an identity element 1
- $x(y+z) = xy + xz \quad \forall x, y, z \in \mathbb{R}$

Examples of rings:

- $\mathbb{Z}$ is a ring
- Every field is a ring, (e.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$)
- $\mathbb{Z}/n \qquad \mathbb{Z}$ modulo $n = \{0, \ldots, n-1\}$
- $\mathbb{F}[\mathrm{X}] = \{$ polynomials $f(x)$ with coefficients in $\mathbb{F}$

1.2 Review

1.2.1 Congruences

Let n be a positive integer. Given $x, y \in \mathbb{Z}$, we say x is congruentt to y modulo n if $x - y$ is a multiple of n.

$$x \equiv y(n) \qquad \text{or} \qquad x \equiv y \bmod n$$

E.g $\quad 2 \equiv 12 \ (10)$
$\qquad\quad \equiv -8 \ (10)$

We write $\mathbb{Z}/n$ for the ring of congruency classes modulo n, i.e. the elements are integer, with two of them regarded as the same if they are congruent modulo n.

Since every integer is congruent to a unique integer in the set $\{0, \ldots, n-1\}$, we have $\mathbb{Z}/n = \{0, \ldots, n-1\}$.

An element x of $\mathbb{Z}/n$ is called "invertible" or a "unit" if $\exists y \in \mathbb{Z}/n$ such that $xy \equiv 1(n)$.

Theorem 1.1. *x is invertible modulo n iff x and n are coprime*

Recall Two numbers are coprime if their highest common factor is 1.

Here's how we find the inverse of x in $\mathbb{Z}/n$. Since X and n are coprime we can find $h, k \in \mathbb{Z}$ such that $hx + kn = 1 \implies hx = 1 \ (n)$. So h is the inverse of x modulo n.

E.g We'll find the inberse of 7 modulo 25 using Euclid's algorithm

$$\begin{aligned} 25 &= 3\times 7+4 \\ 7 &= 1\times 4+3 \\ 4 &= 1\times 3+1 \end{aligned} \qquad \begin{aligned} 1 &= 4-1(3) \\ 1 &= 4-1(7-1(4)) = 2(4)-1(7) \\ 1 &= 2(25-3(7))-1(7) = 2(25)-7(7) \end{aligned}$$

$$\begin{aligned} 2(25)-7(7) &= 1 \\ -7(7) &= 1 \ \ (25) \end{aligned}$$

$$\begin{aligned} (7^{-1}) &= -7 = 18 \ \ (25) \\ 7\times 18 &= 126 = 1 \ \ (25) \end{aligned}$$

We'll write $(\mathbb{Z}/n)^{\times}$ for the invertible elements in $\mathbb{Z}/n$

E.g
$(\mathbb{Z}/3)^{\times} = \{\ \cancel{0},\ 1,\ 2\ \}$
$(\mathbb{Z}/6)^{\times} = \{\ \cancel{0},\ 1,\ \cancel{2},\ \cancel{3},\ \cancel{4},\ 5\ \}$

Theorem 1.2. $(\mathbb{Z}/n)^{\times}$ *is a group with the operation of multiplicity.*

1.2.2 Solving Linear Congruences

Suppose we want to solve $ax \equiv b \ (n)$ (given a, b and n).

Case 1: If a is coprime to n then we can find a^{-1} modulo n by Euclid's algorithm,
$x \equiv a^{-1}b \ (n)$

Case 2: If a is a factor of n, then there are two possibilities:
2a) if a is also a factor of b then $ax \equiv b \quad (n)$ is equivalent to $x = \frac{b}{a} \quad (\frac{n}{a})$
2b) if a is not a factor of b then there are no solutions

E.g. Solve $5x = 11 \ (13)$
This is case 1 because 5 and 13 are coprime

$$\begin{aligned} 13 &= 2 \times 5 + 3 & 1 &= (3) - 1(2) \\ 5 &= 1 \times 3 + 2 & 1 &= (3) - 1(5 - 1(3)) = 2(3) - (5) \\ 3 &= 1 \times 2 + 1 & 1 &= 2(13 - 2(5)) - (5) = 2(13) - 5(5) \end{aligned}$$

$$\begin{aligned} 1 &\equiv -5(5) \quad (13) \\ 5^{-1} &\equiv -5 \equiv 8 \quad (13) \end{aligned}$$

$$\begin{aligned} 5x \equiv& 11 \quad (13) \\ x \equiv 8 \times 11 \equiv& 88 \quad (13) \end{aligned}$$

$$x \equiv 10 \quad (13)$$

E.g. Solve $7x \equiv 84 \quad (490)$
7 is a factor of 490 so case 2)
7 is a factor of 84 so case 2a)

$7x \equiv 84 \quad (490)$
$x \equiv 12 \quad (70)$

E.g. Solve $7x \equiv 85 \quad (490)$
This is case 2b (7 is a factor of 490 but not of 85) $\therefore$ No solutions

$7x \equiv 85 \quad (490)$
$\implies 7x = 85 + 490y$ for some $y \in \mathbb{Z}$
$\implies 0 \equiv 1 \quad (7)$

E.g. Solve $6x \equiv 3 \quad (21)$
This is neither case 1 nor case 2 but we can rewrite as:

$3(2x) \equiv 3 \quad (21)$

By case 2 we can solve for $2x \equiv 1 \quad (7)$
but now 2 is invertible modulo 7 so now solve by case 1

$\therefore x \equiv 4 \quad (7)$

1.3 Chinese Remainder Theorem

Suppost we know the congruency class of x modulo 10. Then we can work out its congruency class mod 2 and mod 5.
E.g. if $x \equiv 7 \ (10)$, then $x \equiv 1 \ (2)$ and $x \equiv 2 \ (5)$

Then the Chinese Remainder Theorem allows us to do the opposite, i.e. if we know x modulo 2 and modulo 5, then we can work out the value of x modulo 10.

Suppose n & m are coprime positive integers, let $a \in (\mathbb{Z}/n)$ and $b \in (\mathbb{Z}/m)$ then there is a unique

$$x \in (\mathbb{Z}/nm) \text{ such that } \begin{aligned} x &\equiv a \quad (n) \\ x &\equiv b \quad (m) \end{aligned}$$

Proof of existence part:
Since n & m are coprime, we can find $h, k \in \mathbb{Z}$ such that $hn + km = 1$.

Let $x = hnb + kma$

Check that this a solution to both congruences:

$$\begin{aligned} &x \equiv kma \quad (n) \\ &x \equiv (1 - hn)a \quad (n) \\ &x \equiv (1)a \quad (n) \\ &x \equiv a \quad (n) \end{aligned}$$

Similarly, this holds for $x \equiv b \quad (m)$.

E.g. Solve the simultaneous congruence:

$$\begin{aligned} &x \equiv 3 \quad (8) \\ &x \equiv 4 \quad (5) \end{aligned}$$

By the Chinese Remainder Theorem, there is unique solution modulo 40. To find the solution we let $x = hnb + kma$.
First find h, k by Euclid's algorithm.

$$\begin{aligned} 8 &= 1 \times 5 + 3 & 1 &= (3) - 1(2) \\ 5 &= 1 \times 3 + 2 & 1 &= (3) - 1(5 - 1(3)) = 2(3) - (5) \\ 3 &= 1 \times 2 + 1 & 1 &= 2(8 - 2(5)) - (5) = 2(8) - 5(5) \end{aligned}$$

$$\begin{aligned} \therefore x &= (2 * 8 * 4) - (3 * 5 * 3) \\ x &= 64 - 45 \\ \implies x &\equiv 19 \quad (40) \end{aligned}$$

Remark: We can use the Chinese Remainder Theorem to solvoe a congruence modulo nm, by first solving mod n and then mod m and then combining the results.
E.g. Solve $x^2 \equiv 2$ (119). Note 119 = 7 * 17.
By CRT this is equivalent to:

$$\begin{aligned} x^2 &\equiv 2 \quad (7) & &\implies x \equiv \pm 3 \quad (7) \\ x^2 &\equiv 2 \quad (17) & &\implies x \equiv \pm 6 \quad (17) \end{aligned}$$

Now we combine the solutions:

$$\begin{aligned} 17 &= 2 * 7 + 3 & 1 &= (7) - 2(3) \\ 7 &= 2 * 3 + 1 & 1 &= (7) - 2(17 - 2(7)) \\ & & 1 &= 5(7) - 2(17) \end{aligned}$$

Since

$$x \equiv \pm 3 \quad (7) \qquad \text{We get } x \equiv 5 * 7 * (\pm 6) - 2 * 17 * (\pm 3)$$
$$x \equiv \pm 6 \quad (17) \qquad x \equiv \pm 11 \text{ or} \pm 45 \quad (119)$$

1.4 Prime numbers

Defintion 1.3. *An integer $p \geq 2$ is a prime number if the only factors of p are $\pm 1, \pm p$*

We'll write $\mathbb{F}_p$ for $\mathbb{Z}/p$. This is because:

Theorem 1.4. *If p is prime, then $\mathbb{F}_p$ is a field*

Proof. Need to check that the non-zero elements of $\mathbb{F}_p$ all have inverses.

Let $x \in \mathbb{F}_p$ with $x \not\equiv 0 \ \ (p)$ i.e. x is not a multiple of p

$\therefore$ hcf$(x, p) = 1$

$\therefore x$ & p coprime $\square$

1.5 Fermat's Little Theorem

Theorem 1.5. *Let p be a prime number. If x is not a multiple of p then $x^{p-1} \equiv 1 \ \ (p)$*

Proof. $x \in \mathbb{F}_p^x = \{1, 2, \ldots, p-1\}$ a group with $p-1$ elements.
Let n be the order of x in this group.
(order of x is smallest $n > 0$ such that $x^n \equiv 1 \ \ (p)$)
By corollary to Lagrange's Theorem, $p-1$ is a multiple of n

$x^n \equiv 1 \ \ (p)$
$x^{p-1} \equiv 1 \ \ (p)$ $\square$

Theorem 1.6. *Lagrange's Theorem: If H is a subgroup of a finite group G, then $|H|$ is a factor of $|G|$.*

Corollary 1.7. *Order of an element is a factor of $|G|$*

We can use Fermat's Little Theorem to do calculations.
E.g. Calculate 10^{100} modulo 19

By Fermat's Little Theorem: $10^{18} \equiv 1 \ \ (19)$

$$\begin{aligned} 10^{100} &\equiv (10^{18})^5 * 10^{10} \quad (19) \\ &\equiv 100^5 \quad (19) \\ &\equiv 5^5 \quad (19) \\ &\equiv 25 * 125 \equiv 6 * 11 \equiv 9 \quad (19) \end{aligned}$$

Also using Fermat's Little Theorem we can solve congruence of the form $x^a \equiv b \ \ (p)$ as long as p prime and a inverible modulo $p-1$

1.5.1 General method to solve $x^a \equiv b \pmod{p}$

Let

$$\begin{aligned} c &= a^{-1} \quad (p-1) \\ ac &= 1 + (p-1)r \end{aligned}$$

Raise both sides of the congruence to power c:

$$\begin{aligned} \therefore x^{ac} &\equiv b^c \quad (p) \\ x^{1+(p-1)r} &\equiv b^c \quad (p) \\ x &\equiv b^c \end{aligned}$$

So the solution is $x \equiv b^c \quad (p)$
E.g. Solve $x^5 \equiv 2 \quad (19)$
19 is prime and 5 is coprime to 18.
Find $c = 5^{-1}$ mod 18

$$\begin{aligned} 18 =& 3 * 5 + 3 \\ 5 =& 2 * 3 - 1 \end{aligned}$$

$$\begin{aligned} 1 =& 2 * 3 - 5 \\ 1 =& 2(18 - 3 * 5) - 5 \\ 1 =& 2 * 18 - 7 * 5 \end{aligned}$$

$$\begin{aligned} \therefore 5^{-1} &\equiv -7 \quad (18) \\ &\equiv 11 \quad (18) \end{aligned}$$

$$\begin{aligned} \therefore x &\equiv 2^{11} \quad (19) \\ &\equiv 2048 \quad (19) \\ &\equiv 15 \quad (19) \end{aligned}$$

1.6 Fundamental Theorem of Arithmetic

If n is a positive integer then there is a unique factorisation, $n = p_1 p_2 \dots p_r$ with p_i prime. "Unique" means up to reordering the primes $p_1, \dots, p_r$. Showing that a factorisation exists is easy. For the uniqueness part we use:

1.6.1 Euclid's Lemma

Lemma 1.8. *Suppose p prime, and $p|ab$. Then $p|a$ or $p|b$.*

To prove Euclid's lemma we use Bezout's lemma.

Proof. Assume $p|ab$ but $p \nmid a$. Then $\mathrm{hcf}(a, p) = 1$
By Bezout's lemma, $\exists h, k$ such that:
$1 = ha + kp$
$b = hab + kpb$ Both hab and kpb are multiples of p.
$\therefore p|b$ □

1.6.2 Checking whether a number is prime

If n is composite then the smallest factor of n is (apart from 1) is a prime number $p \leq \sqrt{n}$, i.e. to show that n is prime, we just need to show that none of the primes up to $\sqrt{n}$ are factors of n.

E.g. Is 199 prime?

$\sqrt{199} < 15$ since $15^2 = 225$

The primes up to 15 are $\cancel{2}, \cancel{3}, \cancel{5}, \cancel{7}, \cancel{1}1, \cancel{1}3$

$199 \equiv 3 \quad (7)$

$199 \equiv 4 \quad (13)$

$\therefore$ 199 is prime

Theorem 1.9. *There are infinitely many primes*

Proof. Suppose $p_1, \ldots, p_n$ are all the primes.

Let $N = p_1 \ldots p_n + 1$

$\therefore N$ has no prime factors $\lightning$ $\square$

Similarly there are infinitely many primes $p \equiv 2 \pmod{3}$

Proof. Assume there are only finitely many primes, call them $p_1, p_2, \ldots, p_r$. All other primes are either 3 or are congruent to 1 mod 3.

Let $N = 3p \ldots p_{r-1}$. Since $3 \not| N$ and $p_i \not| N$ then all the prime factor of N are congruent to 1 mod 3.

$\therefore N \equiv 1 \quad (3) \implies$ because clearly $N \equiv 2 \quad (3)$ $\square$

2 Elementary Number Theory

2.1 Euler Totient Function

Recall $(\mathbb{Z}/n)^\times$ is the group of invertible elements in $\mathbb{Z}/n$.
E.g. $(\mathbb{Z}/6)^\times = \{1, 6\}$
$(\mathbb{Z}/8)^\times = \{1, 3, 5, 7\}$
These are groups with the multiplication operation, * . The multiplication table for $(\mathbb{Z}/8)^\times$ is given below.

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Defintion 2.1. *The Euler Totient function is* $\phi(n) = |(\mathbb{Z}/n)^\times|$

E.g. $\phi(6) = 2$
$\phi(8) = 4$

If p prime then $(\mathbb{Z}/p)^\times = \{1, \ldots, p-1\}$ so $\phi(p) = p - 1$

Theorem 2.2. *Euler's Theorem- Let* $x \in (\mathbb{Z}/n)^\times$ *then* $x^{\phi(n)} \equiv 1 \pmod{n}$

In the case $n = p$ is prime, this is just Fermat's Little Theorem.

Proof. Let d be the order of x, i.e. $x^d \equiv 1 \pmod{n}$. By a corollary to Lagrange's Theorem, d is a factor of $\phi(n) \implies x^{\phi(n)} \equiv 1 \pmod{n}$ □

We can use Euler's theorem to solve congruences and calculate powers mod n. To use the theorem, we need a quick way of calculating $\phi(n)$.

Lemma 2.3. *Let* $n = p^a$ *where* p *is prime* $a > 0$. *Then* $\phi(n) = (p-1)p^{a-1}$

E.g. $\phi(8) = \phi(2^3) = (2-1)2^{3-1} = 4$

Proof. An integer is coprime to p^a as long as it's not a multiple of p.
$\therefore$ The elements of $\mathbb{Z}/p^a$ which are not invertible are the multiples of p. $0, p, 2p, \ldots, p^a - p$.
There are $p^a - 1$ of these:

$\therefore |(\mathbb{Z}/p^a)^\times| = p^a - p^{a-1} = (p-1)p^{a-1}$ □

Theorem 2.4. *Let* n *and* m *be coprime. Then there is an isomorphism:*

$$(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times$$

We'll use the theorem before we prove it.
Remark: If G and H are groups, $G \times H = \{(x, y) : x \in G, y \in H\}$, then $G \times H$ is a group with the operation , $(x, y)(x', y') = (xx', yy')$ and $G \times H$ is the "direct product" of G and H

Corollary 2.5. *If n and m are coprime then $\phi(nm) = \phi(n)\phi(m)$*

Proof.

$$\begin{aligned}\phi(nm) = |(\mathbb{Z}/n)^\times| &= |(\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times| \\ &= |(\mathbb{Z}/n)^\times| * |(\mathbb{Z}/m)^\times| \\ &= \phi(n)\phi(m)\end{aligned}$$

□

Corollary 2.6. *(Corollary of the corollary): Suppose $n = p_1^{a_1} \dots p_r^{a_r}$ with $p_1, \dots p_r$ distinct primes and $a_i > 0$. Then*

$$\phi(n) = (p_1 - 1)p^{a_1 - 1} \; * \cdots * \; (p_r - 1)p_r^{a_r - 1}$$

Proof. Since $p_1^{a_1}, \dots, p_r^{a_r}$ are coprime,

$$\begin{aligned}\phi(n) &= \phi(p_1^{a_1}) \dots \phi(p_r^{a_r}) && \text{by the corollary} \\ &= (p_1 - 1)p_1^{a_1 - 1} \dots (p_r - 1)p_r^{a_r - 1} && \text{by the lemma}\end{aligned}$$

□

E.g. Calculate $\phi(200)$

$$\begin{aligned}\phi(200) &= \phi(2^3 * 5^2) \\ &= (2-1)2^{3-1} * (5-1)5^{2-1} \\ &= 4 * 4 * 5 \\ &= 80\end{aligned}$$

Theorem 2.7. *Suppose n and m are coprime, then $(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times$*
The isomorphism is the map $x \mapsto (x \mod n, x \mod m)$

E.g. $n = 4$, $m = 5$

$$\begin{aligned}(\mathbb{Z}/4)^\times &= \{1, 3\} \\ (\mathbb{Z}/5)^\times &= \{1, 2, 3, 4\} \\ \therefore (\mathbb{Z}/4)^\times * (\mathbb{Z}/5)^\times &= \{(1,1), (1,2), (1,3), (1,4), \\ &\quad\;\; (3,1), (3,2), (3,3), (3,4)\} \\ (\mathbb{Z}/20)^\times &= \{1, 3, 7, 9, 11, 13, 17, 19\}\end{aligned}$$

The isomorphism is:

$$\begin{aligned}1 &\mapsto (1,1) & 11 &\mapsto (3,1) \\ 3 &\mapsto (3,3) & 13 &\mapsto (1,3) \\ 7 &\mapsto (3,2) & 17 &\mapsto (1,2) \\ 9 &\mapsto (1,4) & 19 &\mapsto (3,4)\end{aligned}$$

Proof. Let $\Phi : \mathbb{Z}/nm \mapsto \mathbb{Z}/n * \mathbb{Z}/m$

$\Phi(x) = (x \mod n, x \mod m)$

This is a bijection by the Chinese Remainder Theorem.

We'll next show that x is invertible mod $nm \iff x$ is invertible mod n and mod m

($\implies$) Suppose x is invertible mod nm

$$\begin{aligned} \text{Let } xy &\equiv 1 \pmod{nm} \\ \therefore xy &\equiv 1 \pmod{n} \\ xy &\equiv 1 \pmod{m} \end{aligned}$$

$\therefore x$ invertible mod n and m

($\impliedby$) Suppose x invertible mod n and m

$$\begin{aligned} xa &\equiv 1 \pmod{n} \\ xb &\equiv 1 \pmod{n} \end{aligned}$$

By the Chinese Remainder Theorem, $\exists y$ such that $y \equiv a \pmod{n}$

$y \equiv b \pmod{m}$

$$\left.\begin{aligned} \therefore xy &\equiv xa \equiv 1 \pmod{n} \\ &\equiv xb \equiv 1 \pmod{m} \end{aligned}\right\} \implies xy \equiv 1 \pmod{nm} \text{ by the Chinese Remainder Theorem}$$

We've shown that Φ gives a bijection between $(\mathbb{Z}/nm)^\times$ and $(\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times$. We'll next check that $\Phi(xy) = \Phi(x)\Phi(y)$.

$$\begin{aligned} \Phi(xy) &= (xy \mod n, xy \mod m) \\ &= (x \mod n, x \mod m) * (y \mod n, y \mod m) \\ &= \Phi(x)\Phi(y) \end{aligned}$$

□

2.2 Euler's Theorem

If $x \in (\mathbb{Z}/n)^\times$ then $x^{\phi(n)} \equiv 1 \pmod{n}$ and $\phi(p_1^{a_1} \dots p_r^{a_r}) = (p_1 - 1)p^{a_1 - 1} \dots (p_r - 1)p_r^{a_r - 1}$

E.g. Calculate $7^{135246872002} \mod 10000$

$$\begin{aligned} &7 \text{ coprime to } 10000 \text{ so } 7^{\phi(10000)} \equiv 1 \pmod{10000} \\ &10000 = 2^4 * 5^4 \\ \therefore &\phi(10000) = (2-1)2^3 * (5-1) * 5^3 = 8 * 500 \\ &7^{4000} \equiv 1 \pmod{10000} \implies 7^n \text{ depends only on } n \text{ mod } 4000 \\ &135246872002 \equiv 2 (4000) \\ \therefore &7^{135246872002} \equiv 7^2 \equiv 49 \pmod{10000} \end{aligned}$$

We can also use Euler's THeorem to solve congruence with powers

2.2.1 Solving equations of the form $x^a \equiv b \pmod{n}$

Supose we want to solve $x^a \equiv b \ (n)$ where b is coprime to n and a is coprime to $\phi(n)$. Clearly any solution x must be coprime to n by Euler's Theorem $x^{\phi(n)} \equiv 1 \ (n)$.
$\therefore$ The congruency class of $x^y \mod n$ depends only $y \mod \phi(n)$

Let

$$c = a^{-1} \mod \phi(n)$$

Raise both sides of the congruence to power c:

$$x^{ac} \equiv x^1 \equiv b^c \ (n)$$

$\therefore$ The solution is $x \equiv b^c \ (n)$

E.g. $x^7 \equiv 3 \ (50)$
3 is coprime to 50,

$$\begin{aligned} 50 &= 2 * 5^2 \\ \implies \phi(50) &= 1 * 4 * 5 = 20 \end{aligned}$$

7 is coprime to $\phi(50)$. To solve, we need to find

$$\begin{aligned} c &\equiv 7^{-1} \mod \phi(50) \\ &\equiv 3 \ (20) \end{aligned}$$

$$x \equiv 3^3 \equiv 27 \ (50)$$

E.g. $x^{27} \equiv 5 \ (123)$
5 is coprime to 123,

$$\begin{aligned} 123 &= 3 * 41 \\ \implies \phi(123) &= 2 * 40 = 80 \end{aligned}$$

27 is coprime to 80
To solve, we find $27^{-1} \mod 80$

$$\begin{aligned} 80 &= 3 * 27 - 1 \\ \implies 1 &= 3 * 27 - 80 \end{aligned}$$

$$27^{-1} = 3$$

$$\begin{aligned} x &= 5^3 \\ x &= 125 \equiv 2 \ (123) \end{aligned}$$

2.3 Primitive roots

Recall, let G be a finite group. G is called a cyclic group if $\exists x \in G$ such that, every element in G has the form x^n for some $n \in \mathbb{Z}$, i.e. $G = \{1, x, x^2, \ldots, x^{n-1}\}$ where n is the order of x, equivalentl the order of x is $|G|$. The element x is called a generator of G.

Theorem 2.8. *(Gauss' Theorem), For ever prime number p, the group $\mathbb{F}_p^\times$ is cyclic*

Defintion 2.9. *A generator of $\mathbb{F}_p^\times$ is called a primitive root. Equivalently, this is an element of order $p-1$*

E.g. $p = 7, x = 3$ We'll see that 3 is a primitive root modulo 7

$$\text{Powers of 3 in } F_7^\times: \quad \begin{array}{ccc} 3^0 = 1 & 3^3 \equiv 6 \pmod{7} & 3^6 \equiv 1 \pmod{7} \\ 3^1 = 3 & 3^4 \equiv 4 \pmod{7} & \\ 3^2 \equiv 2 \pmod{7} & 3^5 \equiv 1 \pmod{7} & \end{array}$$

so 3 is a primitive root modulo 7. There is a quicker way to check whether x is a primitive root.

Proposition 2.10. *Let $x \in \mathbb{F}_p^\times$, then x is a primitive root modulo p if and only if for every prime factor q of $p-1$:*

$$x^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

Proof. Assume the second statement is false, so $\exists$ prime factor q of $p-1$ such that:

$$x^{\frac{p-1}{q}} \equiv 1 \pmod{p} \qquad \therefore \text{order of } x \leq \frac{p-1}{q} < p-1$$

$$\therefore x \text{ is not a primitive root}$$

Conversely, assume x is not a primitive root, so x doe not have order $p-1$. But the order of x is a factor of $p-1$.
Suppose the order of x is $\frac{p-1}{d}$, $d > 1$.
Let q be a prime factor of $d \implies q | p-1$
$\frac{p-1}{q}$ is a multiple of $\frac{p-1}{d}$ but $x^{\frac{p-1}{q}} \equiv 1 \pmod{p} \implies x^{\frac{p-1}{q}} \equiv 1 \pmod{p}$

□

E.g. $p = 29$
By the proposition x is a primitive root mod 29 $\iff x^{28/2} \not\equiv 1 \pmod{29}$ and $x^{28/7} \not\equiv 1 \pmod{29}$

$$\iff x^{14} \not\equiv 1 \pmod{29} \text{ and } x^4 \not\equiv 1 \pmod{29}$$

$$\text{Try } x = 2: \quad \begin{array}{c} 2^4 \equiv 16 \not\equiv 1 \pmod{29} \\ 2^{14} \equiv 128^2 \equiv 12^2 \equiv 144 \equiv -1 \pmod{29} \end{array}$$

$\therefore$ 2 is a primitive root mod 29

Another trick to speed up the calculation:
$\mathbb{F}_p$ is a field $\therefore$ every polynomimal of d has no more than d in $\mathbb{F}$ (proved in 2201).
$\therefore$ if $x^2 \equiv 1 \pmod{p}$ then $x \equiv \pm 1 \pmod{p}$

This means that checking whether $x^{14} \equiv 1 \ (29)$ is equivalent to checking whether $x^7 \equiv \pm 1 \ (29)$.

E.g 3 is also a primitive root modulo 29

$$3^2 \equiv 9 \not\equiv \pm 1 \ \ (29)$$
$$3^4 \equiv 1 \ \ (29)$$

$$\begin{aligned} 3^7 &\equiv 27^2 * 3 \ \ (29) \\ &\equiv (-2)^2 * 3 \equiv 12 \ \ (29) \\ &\equiv \pm 1 \ \ (29) \end{aligned}$$

$$\therefore 3^{14} \not\equiv 1 \ \ (29)$$

2.4 Roots of unity and Cyclotomic Polynomials

A complex number ζ is called an n^{th} root of unity if $\zeta^n = 1$. The n^{th} roots of unity are $e^{2\pi i \frac{a}{n}}$ for $a = \{0, 1, \ldots, n-1\}$
We call ζ a primitive n^{th} root of unity if n smaller power than ζ^n is equal to 1, i.e. ζ has order n in $\mathbb{C}^\times$ if ζ is not a primitive n^{th} root of unity $\zeta = e^{2\pi i \frac{b}{d}}$ where $b = \{0, \ldots, d-1\}$ for $d < n$
$\therefore \frac{a}{n} = \frac{b}{d}$

The cancellation happens when a is not coprime to n. This shows that the primitive n^{th} of unity are $e^{2\pi i \frac{a}{n}}$, $a \in (\mathbb{Z}/n)^\times$.

Corollary 2.11. *There are exactly $\phi(n)$ primitive n^{th} roots of unity*

We'll actually prove a more precise version of Gauss' Theorem.

Theorem 2.12. *For every factor d of p^{-1} there are $\phi(d)$ elements in $\mathbb{F}_p^\times$ of order d.*

Defintion 2.13. *The n^{th} cyclotomic polynomial is:*

$$\Phi_n(x) = \Pi_{\substack{primtive \\ n^{th} roots \\ of\ unity\ \zeta}} (X - \zeta)$$

i.e $\zeta^n = 1$ and no smaller power of ζ is 1, $\zeta = e^{2\pi i \frac{a}{n}}, a \in (\mathbb{Z}/n)^\times$

This has degree $\phi(n)$.

E.g. n=4
Primitive 4^{th} roots of unity are $i, -i$:

$$\begin{aligned}\Phi_4(x) &= (x-i)(x-(-i)) \\ &= x^2+1\end{aligned}$$

Lemma 2.14. *For every $n > 0$:*

$$x^n - 1 = \Pi_{\substack{factors \\ d\ of\ n}} \Phi_d(x)$$

E.g. Calculate $\Phi_6(x)$

By the lemma

$$x^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6 \qquad x^6 - 1 = (x^3-1)\Phi_2\Phi_6$$

$$x^3 - 1 = \Phi_1\Phi_3$$

$$\therefore \Phi_6 = \frac{x^6-1}{(x^3-1(x+1)} = \frac{x^3+1}{x+1} = x^2 - x + 1$$

Let p be a prime number. A primitive root mod p is an $x \in \mathbb{F}_p^\times$, such that x generates $\mathbb{F}_p^\times$. Equivalently order $= p-1$

2.4.1 How to calculate $\Phi_n(x)$

Lemma 2.15. $x^n - 1 = \Pi_{d|n}\Phi_d(x)$

E.g. $n = 4$

$$x^4 - 1 = \Phi_1\Phi_2\Phi_4 \qquad \begin{aligned}\Phi_1 &= x-1 \\ \Phi_2 &= (x-(-1)) = x+1 \\ \Phi_4 &= (x-i)(x-(-i)) = x^2+1\end{aligned}$$

$$= (x-1)(x+1)(x^2+1)$$

Proof.

$$x^n - 1 = \Pi_{\substack{\zeta \text{ is an} \\ n^{th} \text{ root of} \\ \text{unity}}} (x-\zeta)$$

but every n^{th} root of unity is a primitive d^{th} root of unity for some $d|n$.

$$x^n = \Pi_{d|n}(\Pi_{\substack{\text{primitive} \\ d^{th}\text{roots} \\ \text{of unity}}}(x-\zeta)) = \Pi_{d|n}\Phi_x(x)$$

$\square$

E.g. Calculate $\Phi_5(x)$

$$\begin{aligned} x^5 - 1 &= \Phi_1(x)\Phi_5(x) \\ &= (x-1)\Phi_5(x) \end{aligned}$$

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4$$

More generally if p prime then $x^p - 1 = (x-1)\Phi_p(x) \implies \Phi_p(x) = 1 + x + \cdots + x^{p-1}$
E.g. Calculate $\Phi_8(x)$

$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$$

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) \implies \Phi_8(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1$$

Corollary 2.16. *$\Phi_n(x)$ has coefficients in $\mathbb{Z}$*

Proof. $\Phi_n(x) = \dfrac{x^n - 1}{\Pi_{\substack{d|n \\ d \neq n}} \Phi_d(x)}$

We'll prove the corollary by induction on n, clearly true when $n = 1$. Assume Φ_d has integer coefficients $\forall d < n$.
It is proved in Algebra 3 (MATH2201) that, if $f, g \in \mathbb{Z}[X]$ and g monic then $f = qg + r$ where $deg(r) < deg(g)$ and $g, r \in \mathbb{Z}[x]$.
Using this, we get that the denominator $\Pi_{\substack{d|n \\ d \neq n}} \Phi_d(x)$ is a monic polynomial with coefficients in $\mathbb{Z} \implies \Phi_n \in \mathbb{Z}[X]$. □

2.4.2 Gauss' Theorem

Theorem 2.17. *Let n be a factor of $p-1$, where p is prime. Then there are exactly $\phi(n)$ elements of order n in $\mathbb{F}_p^\times$. These are the roots of Φ in $\mathbb{F}_p^\times$. In particular there are $\phi(p-1)$ primitive roots.*

Proof. Let $f(x) = x^{p-1} - 1$
By Fermat's Little theorem, $f(x) = 0 \ \ (p)$ for $x = 1, \ldots, p-1$ for $(x \neq 0)$

$$\begin{aligned} \therefore f(x) &= (x-1)(x-2)\ldots(x-(p-1)) \\ &= \Pi_{n|p-1}\Phi_n(x) \end{aligned}$$

This implies that:

- Each Φ_n (for $n|p-1$) factorises completely into linear factors with no repeated roots $\therefore \Phi_n$ has $\phi(n)$ roots in $\mathbb{F}_p$
- Every element of $\mathbb{F}_p^\times$ is a root of exactly one of the polynomials Φ_n with $n|p-1$

It remains to show that the roots of $\Phi_n(x)$ in $\mathbb{F}_p$ has order of exactly n.
Suppose $\Phi_n(x) \equiv 0 \pmod p$

By the lemma $\Phi_n(x)$ is a factor $x^n - 1$

$$\therefore x^n - 1 \equiv 0 \pmod p$$
$$\therefore x^n \equiv 1 \pmod p$$

Suppose $x^m \equiv 1 \pmod p$ for some $m|n$, $m < n$

$$\implies x^m - 1 \equiv 0 \pmod p$$

By the lemma $\Pi_{d|m}\Phi_d(x) \equiv 0 \pmod p$

$$\implies \Phi_d(x) \equiv 0 \pmod p \text{ for some } d \quad \lightning$$

We already know that x is only a root of 1 of the cyclotomic polynomials, therefore x has order n. ☐

2.5 Quadratic reciprocity (Quadratic equations modulo prime numbers)

Recall we can solve $x^a \equiv b \pmod p$ as long as a is coprime to $p-1$. This won't work if $a = 2$ because a will not be invertible mod $p-1$. An easier question to ask is, which quadratic equations have solutions modulo p?
E.g. Does $x^2 \equiv 37 \pmod{149}$ have solutions?

Notation: We always let p be an odd prime (i.e. $p \neq 2$)

An element $a \in \mathbb{F}_p^\times$ is a quadratic residue if $x^2 \equiv a \pmod p$ has solutions.
An element $a \in \mathbb{F}_p^\times$ is a quadratic non-residue if there are no solutions.

The quadratic residue symbol is defined for $a \in \mathbb{F}_p^\times$ by

$$(\frac{a}{p}) = \begin{cases} 1 & \text{a quadratic residue} \\ -1 & \text{a quadratic non-residue} \end{cases}$$

Lemma 2.18. *Let g be a primitive root modulo p (p odd prime). Then g^r is a quadratic residue iff r even.*

Proof.

$(\impliedby)$Assume r even

Clearly g^r is a square in $\mathbb{F}_p^\times$

So g^r is a quadratic residue

$(\implies)$Assume $g^r \equiv x^2 \pmod p$

$x \equiv g^s \pmod p$ $\quad (s \in \mathbb{Z})$ since g primitive roots

$\therefore g^r \equiv g^{2s} \pmod p$

$g^{r-2s} \equiv 1 \pmod p$

g has order $p-1$,so $r-2s$ is a multiple of $p-1$

p odd $\implies p-1$ is even $\implies r$ is even

☐

E.g. $p = 7$

x	$x^2 \mod 7$
± 1	1
± 2	4
± 3	2

$\implies$

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

So 1,2,4 are quadratic residues; 3,4,6 are quadratic non-residues

Corollary 2.19. *There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues mod p*

Defintion 2.20. *Euler's criterion: Let p be an odd prime and $a \in \mathbb{F}_p^\times \implies (\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$*
Also $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

Proof. $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$ by Fermat's Little theorem.

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

Let $a = g^r$ where g is a primitive root $\implies a^{\frac{p-1}{2}} \equiv g^{(p-1)\frac{r}{2}}$

$$\begin{aligned} a \text{ is a quadratic residue} &\iff r \text{ is even} \\ &\iff (p-1)\frac{r}{2} \text{ is a multiple of } p-1 \\ &\iff g^{(p-1)\frac{r}{2}} \equiv 1 \pmod{p} \\ &\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \end{aligned}$$

□

To calculate $(\frac{a}{p})$, we'll use three theorems:

2.5.1 Quadratic Reciprocity Law

Let p, q be distinct odd prime numbers. Then $(\frac{p}{q}) = (-1)^{\frac{(p-1)(q-1)}{4}}$

$$\text{i.e. } (\frac{p}{q}) = \begin{cases} (\frac{q}{p}) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -(\frac{q}{p}) & \text{if } p \equiv q \equiv -1 \pmod{4} \end{cases}$$

2.5.2 First Nebensatz

If p is an odd prime, then $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

$$\text{i.e. } (\frac{-1}{p}) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv -1 \pmod{4} \end{cases}$$

2.5.3 Second Nebensatz

Let p be an odd prime, then $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

$$\text{i.e. } (\frac{2}{p}) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

We'll prove the theorems later.

E.g. Does the congruence $x^2 \equiv 37 \ \ (199)$ have solutions?

$$\begin{aligned}
199 \text{ is an odd prime } (\frac{37}{199}) &= +(\frac{199}{37}) && \text{by quadratic reciprocity} \\
&\equiv (\frac{14}{37}) && \text{because } 199 \equiv 14 \ \ (37) \\
&\equiv (\frac{2}{37})(\frac{7}{37}) && \text{by the corollary} \\
&\equiv (-1)(\frac{7}{37}) && \text{by the } 2^{nd} \text{ Nebensatz} \\
&\equiv (-1)(+1)(\frac{37}{7}) && \text{by the quadratic reciprocity law} \\
&\equiv -(\frac{2}{7}) && \text{because } 37 \equiv 2 \ \ (7) \\
&\equiv -(+1) && \text{by the } 2^{nd} \text{ Nebensatz} \\
&\equiv -1 && \therefore x^2 \equiv 37 \ \ (199) \text{ has no solutions}
\end{aligned}$$

E.g. $x^2 \equiv 47 \ \ (53)$ have solutions?

$$(\frac{47}{53}) = +(\frac{53}{47}) = (\frac{6}{47}) = (\frac{2}{47})(\frac{3}{47}) = (+1)(-1)(\frac{47}{3}) = -(-\frac{1}{3}) = -(-1) = +1$$

This shows that 47 is a quadratic residue mod 53, so $x^2 \equiv 47 \ \ (53)$ does have solutions. $(x = 10)$

We can speed up the test for primitive roos using quadratic reciprocity,

$$x \text{ is a primitive root mod } p \iff \forall q | p-1, q \text{ prime } x^{\frac{p-1}{q}} \not\equiv 1 \ \ (p)$$

This means we need to calculate $x^{\frac{p-1}{q}} \ \ (p)$ for primes $q|p-1$, the biggest power of x to calculate is $x^{\frac{p-1}{2}}$. But we can calculate this, because it is $(\frac{x}{p})$ by Euler's criterion.

E.g. Is 35 a primitive root modulo 83?

The primes q dividing 82 are $2, 41$, need to check $35^2, 35^{41}$
$35^2 \not\equiv 1 \ \ (83)$ because $35 \not\equiv \pm 1 \ \ (83)$, a quadratic equation cannot have more than 2 roots.
$35^{41} \equiv (\frac{35}{83}) \ \ (83) = (\frac{5}{83})(\frac{7}{83}) = (\frac{83}{5})(-1)(\frac{83}{7}) = (\frac{3}{5})(-1)(\frac{-1}{7}) = (\frac{5}{3})(-1)(-1) = (\frac{2}{3})$
$= -1 \not\equiv 1 \ \ (83)$
So 35 is a primitive root modulo 83.

Proof. First Nebensatz:
By Euler's criterion, $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \ \ (p)$.
Both sides are ± 1, and $+1 \not\equiv -1 \ \ (p)$ because $p \geq 3 \implies$ they are equal. $\square$

E.g. Find the first primitive root modulo 41
$40 = 2^3 * 5$

$$x \in \mathbb{F}_{41}^{\times} \text{ is a primitive root } \iff \begin{cases} x^{\frac{40}{2}} \not\equiv 1 \ \ (41) \\ x^{\frac{40}{5}} \not\equiv 1 \ \ (41) \end{cases}$$

$$\text{We can then simplify the conditions to: } \begin{cases} \frac{x}{41} = -1 \\ x^4 \not\equiv \pm 1 \ \ (41) \end{cases}$$

Try $x = 2$: $(\dfrac{2}{41}) = 1 \implies$ not a primitive root

Try $x = 3$: $(\dfrac{3}{41}) = (\dfrac{41}{3}) = (\dfrac{2}{3}) = -1$ and $3^4 = 81 \equiv -1 \ \ (41) \implies$ not a primitive root

Try $x = 4$: $\implies$ not a primitive root

Try $x = 5$ $(\dfrac{5}{41}) = (\dfrac{41}{5}) = (\dfrac{1}{5}) = 1 \implies$ not a primitive root

Try $x = 6$: $(\dfrac{6}{41}) = (\dfrac{2}{41})(\dfrac{3}{41}) = 1 * -1 = -1$
$2^4 * 3^4 = -2^4 \equiv 16 \ \ (41) \not\equiv \pm 1 \implies$ so 6 is a primitive root

E.g. For which primes p does the congruence $x^2 \equiv -3 \ \ (p)$ have solutions?

Notice $x = 1$ is a solution mod 2,
$x = 2$ is a solution mod 3.
For primes $p \neq 2, 3$ it depends on $(\frac{-3}{p})$

We'll calculate $(\dfrac{-3}{p})$

$$\begin{aligned}(\frac{-3}{p}) &= (\frac{-1}{p})(\frac{3}{p}) \\ &= (-1)^{\frac{p-1}{2}}(\frac{3}{p}) \\ &= (-1)^{\frac{(3-1)(p-1)}{4}}(\frac{p}{3}) \\ &= (\frac{p}{3})\end{aligned}$$

List the squares mod 3, $1^2 = 1 \ \ (3), 2^2 = 1 \ \ (3)$

$$\therefore (\frac{p}{3}) = \begin{cases} 1 & \text{if } p \equiv 1 \ \ (3) \\ -1 & \text{if } p \equiv 2 \ \ (3) \end{cases}$$

We've shown that $x^2 \equiv -3 \ \ (p)$ has solutions iff $p \neq 2$ or $p \equiv 1 \mod 3$.

Corollary 2.21. *There are infinitely many primes $p \equiv 1 \ \ (3)$*

Proof. Assume there are only finitely many, and call them $p_1, p_2, \dots, p_r$
Let $N = n^2 + 3$ where $n = 2p_1 \dots p_r$
Take a prime factor q of N

$N \equiv 0 \pmod{q}$
$n^2 + 3 \equiv 0 \pmod{q}$
$n^2 \equiv -3 \pmod{q}$
We've just shown that this implies $q = 2$ or 3 or $q \equiv 1 \pmod{3}$ but $q \neq 2, 3, q \not\equiv 1 \pmod{3}$ ↯ $\square$

Before we prove the 2^{nd} Nebensatz, we need to know about a new ring.

Let $\zeta = e^{\frac{2\pi i}{8}}$, a primitive 8^{th} root of unity.
We'll use the ring $\mathbb{Z}[\zeta] = \{f(\zeta) \colon f \in \mathbb{Z}\} = \{a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_n\zeta^n : a_i \in \mathbb{Z}\}$
This is clearly a ring (closed under +,*).

2.6 Uniqueness Lemma

Every $A \in \mathbb{Z}[\zeta]$ can be written uniquely as $A = W + x\zeta + y\zeta^2 + z\zeta^3$ with $w, x, y, z \in \mathbb{Z}$.
We'll use congruence modulo p in the ring $\mathbb{Z}[\zeta]$ to prove the 2^{nd} Nebensatz.

Defintion 2.22. *Let $A, B \in \mathbb{Z}[\zeta]$*
We'll say $A \equiv B \pmod{p\mathbb{Z}[\zeta]}$ if $A - B = pC$ for some $c \in \mathbb{Z}[\zeta]$

$$\begin{aligned}\text{Suppose } A &= a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \\ B &= b_0 + b_1\zeta + b_2\zeta^2 + b_3\zeta^3 \\ C &= c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3\end{aligned}$$

The equation $A - B = pC$ is equivalent (by uniqueness lemma) to:

$$\begin{aligned}a_0 - b_0 &= pC_0, \\ a_1 - b_1 &= pC_1, \\ a_2 - b_2 &= pC_2, \\ a_3 - b_3 &= pC_3,\end{aligned}$$

This implies that the congruence $A \equiv B \pmod{p\mathbb{Z}[\zeta]}$ is equivalent to $a_i \equiv b_i \pmod{p}$ for $i = 0, 1, 2, 3$

Corollary 2.23. $1 \not\equiv -1 \pmod{p\mathbb{Z}[\zeta]}$ *if p is an odd prime.*

This means that to calculate $(\frac{2}{p})$ it is enough to calculate its congruency class mod $(p\mathbb{Z}[\zeta])$
The uniquess lemma is implied by a more general result:

2.6.1 General Uniqueness Lemma

Let $m \in \mathbb{Z}[X]$ be monic and irreducible over $\mathbb{Q}$ of degree d. If $\alpha \in \mathbb{C}$ is a root of m, then every element of $\mathbb{Z}[\alpha]$ can be written uniquely as $a_0 + a_1 + \dots + a_{d-1}\alpha^{d-1}$ with $a_i \in \mathbb{Z}$.
The uniqueness lemma for $\mathbb{Z}[\zeta]$ follows because ζ is a root of $m(x) = \Phi_8(x) = x^4 + 1$. It is proved in (7202 Groups & Rings) that $x^4 + 1$ is irreducible over $\mathbb{Q}$.

Proof. (General Uniqueness Lemma)

Let $A \in \mathbb{Z}[\alpha]$ and $m(\alpha) = 0$

Existence: $A = f(\alpha)$ for some $f \in \mathbb{Z}[X]$

divide f by m with remainder, $f = q * m + r$ $\quad deg(r) < deg(m) < d$

$\therefore \quad f(\alpha) = q(\alpha)m(\alpha) + r(\alpha)$

$\therefore \quad A = r(\alpha)$

Uniqueness: Suppose $A = f(\alpha) = g(\alpha)$ $(f \neq g)$ where f & g both have degree $< d$

$\therefore \quad h(\alpha) = 0$ where $h = f - g$ $(\neq 0)$

m is irreducible over $\mathbb{Q}$ and has a bigger degree than h

$\therefore \quad m \nmid h$ in $\mathbb{Q}[x]$, so m and h are coprime in $\mathbb{Q}[x]$

$\exists a, b \in \mathbb{Q}[x]$ such that :

$1 = am + bh = a(\alpha)m(\alpha) + b(\alpha)h(\alpha) = 0$ $\quad m(\alpha) = 0 \quad h(\alpha) = 0$

$\implies 1 = 0$

$\implies f = g$

□

Lemma 2.24. *In any ring R with any prime p*

$$(x+y)^p \equiv x^p + y^p \ \ (pR) \text{ for any } x, y \in R$$

Proof. Sufficient to show that each binomial coefficient:

$$c = \frac{p!}{i!(p-i)!} \qquad i = 1, 2, \ldots, p-1 \text{ is a multiple of p}$$

$$i!(p-i)! \not\equiv 0 \ \ (p) \implies \in \mathbb{F}_p^\times$$

□

Proof. 2^{nd} Nebensatz

Let p be an odd prime and let $G = \zeta + \zeta^{-1} = \sqrt{2}$. We'll calculate G^p *mod* $(p\mathbb{Z}[\zeta])$ in two ways.
First Calculation:

$$\begin{aligned} G^P &= (\zeta + \zeta^{-1})^p \\ &= \zeta^p + \zeta^{-p} \quad \text{mod } (p\mathbb{Z}[\zeta]) \text{ by the lemma} \end{aligned}$$

Since $\zeta^8 = 1$ this only depends p modulo 8 if $p \equiv \pm 1(8)$ then,

$$G^p = \zeta + \zeta^{-1} \equiv G \ \ (p\mathbb{Z}[\zeta])$$

If $p \equiv \pm 3 \ \ (8)$ then,

$$G^p \equiv \zeta^3 + \zeta^{-3} \equiv -G \ \ (p\mathbb{Z}[\zeta])$$

So in summary,

$$G^p \equiv (-1)^{\frac{p^2-1}{8}} G \ \ (p\mathbb{Z}[\zeta])$$

Second Calculation:

Since $G^2 = 2$,

$$\begin{aligned} G^p &= G * 2^{\frac{p^2-1}{2}} \\ &= G * (\frac{2}{p}) \ \ (p\mathbb{Z}[\zeta]) \text{ by Euler's criterion} \end{aligned}$$

Comparing the results of these two calculations we get:

$$(\frac{2}{p})G = (-1)^{\frac{p^2-1}{8}} G \ \ (p\mathbb{Z}[\zeta])$$

Note $G^2 * \frac{p+1}{2} \equiv 1 \ \ (p\mathbb{Z}[\zeta])$, i.e. G is invertible modulo $p\mathbb{Z}[\zeta]$ with inverse $G * \frac{p+1}{2}$

$$\implies (\frac{2}{p}) \equiv (-1)^{\frac{p^2-1}{8}} \ \ (p\mathbb{Z}[\zeta])$$

Since $1 \equiv -1 \ \ (p\mathbb{Z}[\zeta])$,

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$$

□

The proof of the 2^{nd} Nebensatz worked because $\sqrt{2} \in \mathbb{Z}[\zeta]$
To prove the quadratic reciprocity law, we'll show that $\sqrt{\pm p})$ is in another cyclotomic ring

Let $\zeta_p = e^{\frac{2\pi i}{p}}$, a primtive p^{th} root of unity. We'll work in the ring modulo $q\mathbb{Z}[\zeta]$.

Defintion 2.25. *The p^{th} Gauss sum (where p is an odd prime):*

$$G(p) = \sum_{a=1}^{p-1} (\frac{a}{p})\zeta_p^a \in \mathbb{Z}[\zeta_p]$$

Lemma 2.26. $G(p)^2 = (-1)^{\frac{p-1}{2}}$

Proof.

$$\begin{aligned} G(p)^2 &= \left(\sum_{a=1}^{p-1}(\frac{a}{p})\zeta_p^a\right)\left(\sum_{b=1}^{p-1}(\frac{b}{p})\zeta_p^b\right) \\ &= \sum_{a,b\in\mathbb{F}_p^\times}(\frac{a}{p})(\frac{b}{p})\zeta_p^a\zeta_p^b \\ &= \sum_{a,b\in\mathbb{F}_p^\times}(\frac{ab}{p})\zeta_p^{a+b} \end{aligned}$$

Let $c \equiv a^{-1}b \pmod p$, as b runs through $\mathbb{F}_p^\times$, so does c

$$\begin{aligned} &= \sum_{a,c\in\mathbb{F}_p^\times}(\frac{a^2}{p})\zeta_p^{a+ac} \\ &= \sum_{c\in\mathbb{F}_p^\times}(\frac{c}{p})\left(\sum_{a=1}^{p-1}(\zeta_p^{1+c})^a\right) \end{aligned}$$

Note the second summation is a geometric progression. Recall that,

$$\sum_{i=1}^{p-1} r^i = \begin{cases} \dfrac{r^p-1}{r-1} & r\neq 1 \\ p-1 & r=1 \end{cases}$$

Summing the geometric progression:

$$\sum_{a=1}^{p-1}\left(\zeta_p^{1+c}\right)^a = \begin{cases} \dfrac{\left(\zeta_p^{1+c}\right)^p - \zeta_p^{1+c}}{\zeta_p^{1+c}-1} & \text{if } c \not\equiv 1 \pmod p \\ p-1 & \text{if } c\not\equiv -1 \pmod p \end{cases}$$

$$= \begin{cases} -1 & c\not\equiv -1 \pmod p \\ p-1 & c\equiv -1 \pmod p \end{cases}$$

$$\therefore G(p)^2 = \sum_{c \in \mathbb{F}_p^\times} (\frac{c}{p})(-1) + p(\frac{-1}{p})$$

$\sum_{c \in \mathbb{F}_p^\times} (\frac{c}{p})(-1) = 0$ since there are $\frac{p-1}{2}$ quadratic residues and quadratic non-residues.

$$\begin{aligned} &= p(\frac{-1}{p}) \\ &= (-1)^{\frac{p-1}{2}} p && \text{by the } 1^{st} \text{ Nebensatz} \end{aligned}$$

□

2.6.2 Uniqueness Lemma for $\mathbb{Z}[\zeta_p]$

Every element $A \in \mathbb{Z}[\zeta_p]$ can be written uniquely as:

$$A = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \qquad \text{with } a_i \in \mathbb{Z}$$

This is because ζ_p is a root of $m(x) = \Phi_p(x) = 1 + x + \cdots + x^{p-1}$. It's proved in 7202 that Φ_p is irreducible over $\mathbb{Q}$.

Proof. Quadratic Reciprocity law

We'll calculate $G(p)^q \ \ (q\mathbb{Z}[\zeta_p])$ in two ways.

First Calculation:

$$\begin{aligned} G(p)^q &= \left(\sum_{a=1}^{p-1} (\frac{a}{p})\zeta_p^a\right)^q \\ &= \sum_{a=1}^{p-1} \left((\frac{a}{p})\zeta_p^a\right)^q \quad (p\mathbb{Z}[\zeta]) \end{aligned}$$

Since q is odd, $(\frac{a}{p})^q = (\frac{a}{p})$

$$G(p)^q \equiv \sum_{a \in \mathbb{F}_p^\times} (\frac{a}{p})\zeta_p^{aq}$$

Let $b \equiv aq \ \ (p)$, and as a runs through $\mathbb{F}_p^\times$ so does b

$$\begin{aligned} G(p)^q &\equiv \sum_{b \in \mathbb{F}_p^\times} (\frac{bq^{-1}}{p})\zeta_p^b \\ &= (\frac{q^{-1}}{p}) \sum_{b \in \mathbb{F}_p^\times} (\frac{b}{p})\zeta_p^b \end{aligned}$$

Note that $G(p) = \sum_{b \in \mathbb{F}_p^\times} (\frac{b}{p}) \zeta_p^b$ which implies,

$$
\begin{aligned}
G(p)^q &\equiv (\frac{q^{-1}}{p}) G(p) \pmod{q\mathbb{Z}[\zeta_p]} \\
&\equiv (\frac{q}{p}) G(p) \pmod{q\mathbb{Z}[\zeta_p]}
\end{aligned}
$$

Second Calculation:

Since $G(p)^2 = (-1)^{\frac{p-1}{2}} p$,

$$
\begin{aligned}
G(p)^q &= G(p) \left((-1)^{\frac{p-1}{2}} p \right)^{\frac{q-1}{2}} \\
&= G(p)(-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}} \\
\therefore G(p)^q &\equiv G(p)(-1)^{\frac{(p-1)(q-1)}{4}} (\frac{p}{q}) \pmod{q\mathbb{Z}[\zeta_p]} \qquad \text{by Euler's criterion}
\end{aligned}
$$

Comparing the two results we get:

$$
(\frac{q}{p}) G(p) \equiv (-1)^{\frac{(p-1)(q-1)}{4}} (\frac{p}{q}) G(p) \pmod{q\mathbb{Z}[\zeta_p]}
$$

We need to check that $G(p)$ is invertible modulo $q\mathbb{Z}[\zeta_p]$,

$G(p)^2 = \pm p$, which is invertible modulo q

$G(p)$ has inverse $G(p) * (\pm p)^{-1} \pmod{q\mathbb{Z}[\zeta_p]}$

$\therefore (\frac{p}{q}) \equiv (-1)^{\frac{(p-1)(q-1)}{4}} (\frac{p}{q}) \pmod{q\mathbb{Z}[\zeta_p]}$

Since $1 \equiv -1 \pmod{q\mathbb{Z}[\zeta_p]}$, it follows that $(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}} (\frac{p}{q})$ $\square$

3 P-adic Number theory

This means methods for congruences modulo p^n, p prime and n large.

If we want to solve $f(x) = 0$, $x \in \mathbb{R}$ we can use the Newton-Raphson method:

- Begin with an "approximate solution" a_0
- Define a sequence recursively $a_{n+1} = a_n - \dfrac{f(a_n)}{f'(a_n)}$

Very often a_n converge to a limit a and $f(a) = 0$.
We can use the same method in number theory for solving congruences. Suppose $f(x)$ is a polynomial with coefficients in $\mathbb{Z}$ and we want to solve $f(x) \equiv 0 \ \ (p^N)$ (p prime, n large)
We can try this:

- Find a solution a_0 to $f(a_0) \equiv 0 \ \ (p^r)$ where r is small
- Define a recursive sequence $a_{n+1} = a_n - \dfrac{f(a_n)}{f'(a_n)}$

If n is large enough, then often $f(a_n) \equiv 0 \ \ (p^N)$

E.g. Let $f(x) = x^2 + 2$, $p = 3$
Suppose we want to solve $x^2 + 2 \equiv 0 \ \ (3^N)$

Let $a_0 = 1 : f(a_0) = 1^2 + 2 = 3 \equiv 0 \ \ (3)$

Define the sequence a_n by $a_{n+1} = a_n = \dfrac{f(a_n)}{f'(a_n)} = a_n - \dfrac{a_n^2 + 2}{2a_n} = \dfrac{a_n}{2} - \dfrac{1}{a_n}$

$$\begin{aligned} a_0 &= 1 \\ a_1 &= \frac{1}{2} - 1 = \frac{-1}{2} \\ a_2 &= \frac{-1}{4} + 2 = \frac{7}{4} \end{aligned}$$

It turns out that $\frac{-1}{2}$ is a solution mod 9 $\implies -1 * 2^{-1} \mod 9$
$\frac{7}{4}$ is a solution mod 81 $\implies 7 * 4^{-1} \mod 9$

$2^{-1} \equiv 5 \ \ (9) \implies a_1 \equiv 4 \ \ (9)$

$4^{-1} \equiv -20 \ \ (81) \implies a_2 = \frac{7}{4} \equiv -140 \equiv 22 \ \ (81)$

a_3 would be a solution mod 3^8.

In this example, we're reducing rational numbers mod p^n not just integers. If $\frac{a}{b}$ is arational numbe,r then we can reduce this modulo p^n as long as b is invertible mod p^n, i.e. when b is not a multiple of p. We'll write:

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$$

$\mathbb{Z}_{(p)}$ is closed under $+, *$, so $\mathbb{Z}_{(p)}$ is a ring contained in $\mathbb{Q}$ containing $\mathbb{Z}$. This is called the "local ring of p" and is the set of rational number which can be reduce modulo p^n $(\forall n)$

Defintion 3.1. *If p is a prime number and $n \in \mathbb{Z}$, then the valuation of n, at p is:*

$$V_p(n) = \begin{cases} max\{a : p^a | n\} & n \neq 0 \\ \infty & n = 0 \end{cases}$$

A simple statement that can be made is, $V_p(nm) = V_p(n) + V_p(m)$. We can also extend V_p to a function on $\mathbb{Q}$, $V_p(\frac{n}{m}) = V_p(n) - V_p(m)$.
With this notation:

$$Z_{(p)} = \{x \in \mathbb{Q} : V_p(x) \geq 0\}$$

$$x \equiv y \quad (p^a) \iff V_p(x - y) \geq a$$

E.g

$$V_2(\frac{7}{12}) = -2 \qquad V_2(\frac{7}{12}) = -1 \qquad V_5(\frac{7}{12}) = 0 \qquad V_7(\frac{-7}{12}) = +1$$

3.1 Hensel's Lemma

Let p be a prime number. Let $f \in \mathbb{Z}_{(p)}[x]$ and $a_0 \in \mathbb{Z}_{(p)}$ such that $f(a_0) \equiv 0 \ \ (p^{2c+1})$ where $c = V_P(f'(a_0))$.
Then if we define $a_{n+1} = a_n - \dfrac{f(a_n}{f'(a_n)}$ then $a_n \in \mathbb{Z}_{(p)}$ and $f(a_n) \equiv 0 \ \ (p^{2c+2^n})$

Proof. We'll prove the following by induction on n

1. $a_n \in \mathbb{Z}_{(p)}$ and $a_n \equiv a_0 \ \ (p^{c+1})$
2. $V_p(f'(a_n)) = c$
3. $f(a_n) \equiv 0 \ \ (p^{2c+2^n})$

If $n = 0$ then the statements 1,2,3 are all true for a by assumption. Now assume 1,2,3 for a_n, we'll prove them for a_{n+1}

Let $a_{n+1} = a_n - \delta$ where $\delta = \dfrac{f(a_n)}{f'(a_n)}$

1:

$$\begin{aligned} V_p(\delta) &= V_p(f(a_n)) - V_p(f'(a_n)) \\ &\qquad\qquad\qquad = c && \text{by } \mathbf{2:} \\ &\geq 2c + 2^n && \text{by } \mathbf{3:} \\ V_p(\delta) &\geq 2c + 2^n - c \\ V_p(\delta) &\geq c + 2^n && \mathbf{(*)} \end{aligned}$$

By **(*)**

$$V_p(\delta) \geq 0 \implies \delta \in \mathbb{Z}_{(p)}$$

$$\therefore a_{n+1} = a_n - \delta \in \mathbb{Z}_{(p)}$$

By **(*)**

$$V_p \geq c+1 \implies \delta \equiv 0 \pmod{p^{c+1}}$$

$$\begin{aligned} a_{n+1} &\equiv a_n \pmod{p^{c+1}} \\ &\equiv a_0 \pmod{p^{c+1}} && \text{by } \mathbf{1} \end{aligned}$$

2: We've shown that $a_{n+1} \equiv a_0 \pmod{p^{c+1}}$

$$\begin{aligned} \therefore \quad f'(a_{n+1}) &\equiv f'(a_0) \pmod{p^{c+1}} \\ &\not\equiv 0 && \text{because } V_p(f'(a_0)) = c \end{aligned}$$

$$\begin{aligned} \text{also } f'(a_{n+1}) &\equiv f'(a_0) \pmod{p^c} \\ &\equiv 0 \pmod{p^c} \end{aligned}$$

because $V_p(f'(a_0)) = c \pmod{p^c}$

$$\therefore V_p(f'(a_{n+1})) = c$$

3: Must show that $f(a_{n+1}) \equiv 0 \pmod{p^{2c+2^{n+1}}}$ □