Math Enrichment
Number Theory

KÂZIM BÜYÜKBODUK

Abstract. These are the notes from my Mathematics Enrichment lectures in November 2023.

1. Modular arithmetic

Suppose a, b, n are integers. We want to solve for x in the congruence

$$ax \equiv b \mod n\,.$$

This amounts to finding $a^{-1}b \mod n$.

This may not be always possible: $2y \equiv 1 \mod 6$ has no solutions, as for a solution, we would have

$$2 \mid 6 \mid 2y - 1$$

which is impossible.

However: $2y \equiv 1 \mod 5$ has a unique solution $\mod 5$: $y \equiv 3 \mod 5$.

The key difference is that

$$\gcd(2, 6) = 2 > 1 \text{ whereas } \gcd(2, 5) = 1\,.$$

1.1. Suppose $(a, n) = d > 1$. Then $a^{-1} \mod n$ does not exist. Namely, there is no integer y so that $ay \equiv 1 \mod n$.

Proof. If otherwise,

$$d \mid n \mid ay - 1, \text{ but also } d \mid a \implies d \mid 1,$$

contradicting that $d > 1$. □

1.2. Let us define

$$\mathrm{Mod}_n^\times = \{a \mod n : a \in \mathbb{Z} \text{ such that } a^{-1} \mod n \text{ exists}\}\,.$$

Namely, $\mathrm{Mod}_n^\times$ consists of "residue classes" $a \mod n$ for which their inverses exist modulo n. Yet in other words, $\mathrm{Mod}_n^\times$ consists of $a \mod n$ such that one can find an integer y with $ay \equiv 1 \mod n$.

1.2.1. $\mathrm{Mod}_n^\times = \{a \mod n : a \in \mathbb{Z} \text{ such that } (a, n) = 1\} =: S$.

Proof. We already saw that LHS is contained in the RHS. We need to prove the opposite containment. To that end, suppose $b \mod n$ belongs to RHS, i.e. $\gcd(b, n) = 1$. We want to prove that $b^{-1} \mod n$ exists, namely that we can find some integer y with $by \equiv 1 \mod n$.

For that purpose, let us consider the map

$$M_b : S \xrightarrow{x \pmod n \mapsto bx \pmod n} S$$

which indeed makes sense since

$$\gcd(b, n) = 1 = \gcd(x, n) \implies \gcd(bx, n) = 1\,.$$

We claim that the map M_b is injective. Indeed,

$$M_b(x_1) = M_b(x_2) \Longleftrightarrow bx_1 \equiv bx_2 \mod n \Longleftrightarrow n \mid b(x_1 - x_2) \Longleftrightarrow n \mid x_1 - x_2 \Longleftrightarrow x_1 \equiv x_2 \mod n$$

where the last equivalence follows from the fact that $\gcd b, n = 1$. This proves that M_b is indeed injective.

Since the set S is finite (note that we are working $\mod n$), it follows that the map M_b is also surjective (therefore bijective). In particular, there exists a unique $y \mod n$ with

$$by \equiv M_b(y \mod n) \equiv 1 \mod n \in S\,.$$

This is what we wanted to prove.

□

This statement is useful because we can easily compute $\gcd(a, n)$ using the Euclidean algorithm.

1.3. **Application: Euler's theorem.** Suppose that $\gcd(a,n)=1$. Then

$$a^{\varphi(n)} \equiv 1 \mod n\,,$$

where

$$\varphi(n) := \#\mathrm{Mod}_n^\times = \#\{a : a \in \mathbb{Z} \text{ such that } 1 \le a \le n \text{ and } (a,n)=1\}\,.$$

Proof. As we saw in the previous proof,

$$a\mathrm{Mod}_n^\times = M_a(\mathrm{Mod}_n^\times) = \mathrm{Mod}_n^\times\,.$$

That shows

$$\prod_{x \in a\mathrm{Mod}_n^\times} x = \prod_{x \in \mathrm{Mod}_n^\times} .$$

But also

$$\prod_{x \in a\mathrm{Mod}_n^\times} x = \prod_{y \in \mathrm{Mod}_n^\times} ay = a^{\varphi(n)} \times \prod_{y \in \mathrm{Mod}_n^\times} y\,.$$

Combining these two equalities, we deduce that

$$a^{\varphi(n)} \times \underbrace{\prod_{y \in \mathrm{Mod}_n^\times} y}_{\Pi} = \prod_{y \in \mathrm{Mod}_n^\times} y\,.$$

This shows

$$n \mid \Pi(a^{\varphi(n)} - 1)\,,$$

and since $\gcd(\Pi, n) = 1$, also that $n \mid a^{\varphi(n)} - 1$. $\square$

2. Chinese Remainder Theorem (CRT)

Suppose that $n_1, \cdots, n_k \in \mathbb{Z}$ are pairwise coprime. Suppose that $a_1, \cdots, a_k \in \mathbb{Z}$ are any k-tuple of integers. Then there exists a unique integer x with $0 \le x < n_1 \cdots n_k$ verifying the following congruences simultaneously:

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_k \mod n_k\,. \end{aligned}$$

Example 2.1. *There exists a unique integer $0 \le x < 15 \times 28 \times 169$ such that*

$$\begin{aligned} x &\equiv 4 \mod 15 \\ x &\equiv 23 \mod 28 \\ x &\equiv 127 \mod 169 \end{aligned}$$

I dare you to prove this by brute force!

Proof of CRT. Let us consider

$$\mathrm{Mod}_n^+ = \{\{0,1,\cdots,n-1\}, + \mod n\} = \{\{a \mod n : a \in \mathbb{Z}\}, + \mod n\}$$

the set of integers modulo n, equipped with addition modulo n. Let us put $N = n_1 \cdots n_k$, and consider the 'diagonal' map[1]

$$\Delta : \mathrm{Mod}_N^+ \xrightarrow{x \mod N \mapsto (x \mod n_1, \cdots, x \mod n_k)} \mathrm{Mod}_{n_1}^+ \times \cdots \mathrm{Mod}_{n_k}^+$$

Our goal[2] is to prove that given $(a_1 \mod n_1, \cdots, a_k \mod n_k)$ on the RHS, one can find x so that $\Delta(x) = (a_1 \mod n_1, \cdots, a_k \mod n_k)$. In other words, we contend to prove that Δ is surjective.

Note that the source of Δ has N elements, and its source has $n_1 \cdots n_k = N$ elements as well. As a result, proving that Δ is surjective is the same as proving Δ is injective. This is what we shall verify.

Suppose that we have

$$(x \mod n_1, \cdots, x \mod n_k) = \Delta(x) = \Delta(y) = (y \mod n_1, \cdots, y \mod n_k)\,,$$

which is equivalent to saying that [3]

$$x \equiv y \mod n_1$$

---

[1]In the example above, $N = 70980$ and the map Δ is given by

$$\Delta : \mathrm{Mod}_{70980}^+ \xrightarrow{x \mod 70980 \mapsto (x \mod 15, x \mod 28, x \mod 169)} \mathrm{Mod}_{15}^+ \times \mathrm{Mod}_{28}^+ \times \mathrm{Mod}_{169}^+\,.$$

[2]In the example above, we want to find x such that $\Delta(x) = (4 \mod 15, 23 \mod 28, 127 \mod 128)$.

[3]In the example above, this would mean

$$x \equiv y \mod 15, x \equiv y \mod 28, x \equiv y \mod 169\,,$$

$$\vdots$$

$$x \equiv y \mod n_k$$

which is to say

$$n_1, \cdots, n_k \text{ all divide } x - y\,.$$

But since $n_1, \cdots, n_k$ are coprime, this the same as requiring that their product

$$N = n_1 \cdots n_k \text{ divides } x - y\,,$$

which exactly means $x \equiv y \mod N$, proving that Δ is injective, as required.

□

2.1. **Example.** Prove that for any integer n, one can find integers a, b such that $4a^2 + 9b^2 - 1$ is divisible by n.

2.1.1. *Proof.* The idea is to work modulo n, and factor n into a product of powers of primes (fundamental theorem of arithmetic), solve for prime powers (that divide n) and finally, use CRT to patch things up.

In other words, let's first try to find integers a_p, b_p with

$$4a_p^2 + 9b_p^2 \equiv 1 \mod p^k\,.$$

Case 1: $n = 2^k$ p=2. We want to find a_2, b_2 with

$$4a_2^2 + 9b_2^2 \equiv 1 \mod 2^k\,.$$

Note that $3^{-1} \mod 2^k$ exists since $\gcd(3, 2^k) = 1$. Set $b_2 \equiv 3^{-1} \mod 2^k$ and $a_2 = 0$.

Case 3: $n = p^k$ p>2. We wish to find integers a_p, b_p with

$$4a_p^2 + 9b_p^2 \equiv 1 \mod p^k\,.$$

Since $\gcd(2, p^k) = 1$, we know that $2^{-1} \mod p^k$ exists. Put $a_p \equiv 2^{-1} \mod p^k$ and $b_p = 0$.

General case: $n = p_1^{k_1} \cdots p_m^{k_m}$**, and** p_i **are pairwise distinct primes**:

For each index $i = 1, \cdots, m$, we have found (a_{p_i}, b_{p_i}) such that

$$4a_{p_i}^2 + 9b_{p_i}^2 \equiv 1 \mod p_i^{k_i}\,.$$

By CRT, we can choose $a, b \in \mathbb{Z}$ (applied twice) with

$$a \equiv a_{p_i} \mod p_i^{k_i}\,, \qquad i = 1, \cdots, m\,,$$
$$b \equiv b_{p_i} \mod p_i^{k_i}\,, \qquad i = 1, \cdots, m\,.$$

Then,

$$4a^2 + 9b^2 \equiv 4a_{p_i}^2 + 9b_{p_i}^2 \equiv 1 \mod \quad \mod p_i^{k_i}, \text{ for all } i = 1, \cdots, m\,.$$

This shows

$$p_i^{k_i} \text{ divides } 4a^2 + 9b^2 - 1 \text{ for all } i = 1, \cdots, m\,.$$

Since $p_1, \cdots, p_m$ are pairwise distinct, this means that their product

$$p_1^{k_1} \cdots p_m^{k_m} = n \text{ divides } 4a^2 + 9b^2 - 1\,.$$

□

3. Quadratic residues

Question 3.1. *What are the squares in* $\mathrm{Mod}_n^\times$*? Namely, describe the subset*

$$\square_n := \{a \in \mathbb{Z} : \gcd(a, n) = 1 \textit{ and } a = x^2 \textit{ for some integer } s\}\,.$$

The elements of $\square_n$ are sometimes called "quadratic residues mod n".

3.1. Suppose that p is an odd prime. We will describe the set of quadratic residues $\square_p$ mod p using the following fact without proof.

---

which is to say

$$15, 28, 169 \text{ all divide } x - y\,.$$

3.1.1. $\mathrm{Mod}_p^\times$ contains a primitive root. Namely, there is an integer g coprime to p such that

$$\mathrm{Mod}_p^\times = \{g \mod p, g^2 \mod p, \cdots, g^{p-1} \equiv 1 \mod p\}$$

where the final congruence is Fermat's little theorem (which follows from Euler's theorem that we discussed earlier).

Example 3.2. *$g = 3$ is a primitive root modulo 17 (why?). In general, it is very difficult to find primitive roots.*

3.1.2. Suppose that g is a primitive root modulo p. Then observe that

$$\square_p \supseteq \{g^2, \cdots, g^{p-1}\} = \text{ even powers of } g\,. \tag{3.1}$$

Lemma 3.3. *$\square_p \supset \{g^2, \cdots, g^{p-1}\}$. In particular, there are $\dfrac{p-1}{2}$ quadratic residues modulp p.*

Proof. In view of the containment (3.1), we need to show that odd powers of g are not squares modulo p.

Suppose on the contrary that $g^{2r+1} \in \square_p$; namely, $x^2 \cong g^{2r+1} \mod p$. Since $(g, p) = 1$, $g^{-1} \mod p$ exists, and we have

$$y^2 \equiv [x(g^{-1})^r]^2 \equiv g \mod p\,.$$

Raise both sides of this congruence to the power $\frac{p-1}{2}$:

$$1 \equiv y^{p-1} \equiv g^{\frac{p-1}{2}} \mod p,$$

which is impossible since g is a primitive root modulo p (why?[4]).

$\square$

It is therefore desirable to know which modulus admits a primitive root. Here's the conclusive statement in this vein:

Theorem 3.4. *$\mathrm{Mod}_n^\times$ has a primitive root, i.e. there exists an integer such that*

$$\mathrm{Mod}_n^\times = \{g, g^2, \cdots, g^{\varphi(n)} \mod n\}$$

if and only if

- *either $n = p^\alpha$ where p is an odd prime and α is a positive integer,*
- *or $n = 2p^\alpha$ where p is an odd prime and α is a positive integer,*
- *$n = 2, 4$.*

3.1.3. *Application: Wilson's theorem.* Let g be a primitive root modulo a prime number p. Note that

$$(p-1)! \equiv \prod_{j=1}^{p-1} g^k = g^{\frac{p(p-1)}{2}} \mod p\,.$$

Note also that $g^{\frac{p-1}{2}} \equiv -1 \mod p$. Indeed, if we put $y := g^{\frac{p-1}{2}} \mod p$, note then that

$$y^2 \equiv 1 \mod p$$

and hence (since p is a prime)

$$p \text{ divides } y-1 \text{ or } y+1\,;$$

in other words,

$$y \equiv 1 \mod p \quad \text{or} \quad y \equiv -1 \mod p\,.$$

To verify our claim, we only need to explain that $g^{\frac{p-1}{2}} \not\equiv 1 \mod p$. This follows from the choice of g as a primitive root (see the footnote).

This shows that

$$(p-1)! \equiv -1 \mod p\,,$$

which is known as Wilson's theorem. There're other proofs of it and you're invited to think about one.

[4] Here's a hint: check that, to say that g is primitive root is the same as requiring that $p-1$ is the smallest among the set of positive integers k for which we have $g^k \equiv 1 \mod p$. In other words:

$$g \text{ is a primitive root} \Longleftrightarrow p-1 = \min\{k \in \mathbb{Z}^+ : g^k \equiv 1 \mod p\}.$$

3.1.4. *Example.* Prove that if $2^a \equiv 2^b \mod 101$ then $a \equiv b \mod 100$.

Proof. $2^a \equiv 2^b \mod 101 \Longleftrightarrow 2^{a-b} \equiv 1 \mod 101$, and $a \equiv b \mod 100 \Longleftrightarrow a - b \equiv 0 \mod 100$. Our problem is therefore equivalent to checking that, on setting $m : a - b$,

$$2^m \equiv 101 \Longleftrightarrow 100 \mid m\,.$$

This is equivalent to checking that 2 is a primitive root modulo the prime 101 (convince yourself why this is so).

To check that, you need to check that $2^d \not\equiv 1 \mod 101$ for positive integers $d \mid 100$ with $d < 100$ (convince yourself why checking this is indeed necessary and sufficient). In other words, you need to check that the set

$$\{2, 2^2, 2^4, 2^5, 2^{10}, 2^{20}, 2^{25}, 2^{50} \mod 101\}$$

does not contain $1 \mod 101$. Do that! $\square$

3.1.5. *Example.* Suppose that p is an odd prime. Find all integers k such that

$$1^k + 2^k + \cdots + (p-1)^k =: S_k$$

is divisible by p.

3.1.6. *Solution.* The idea is that calculating the sum of geometric sequences is easy:

$$(1-x)(1 + x + \cdots + x^m) = 1 - x^{m+1} \quad \Longrightarrow \quad (1 + x + \cdots + x^m) = \frac{1 - x^{m+1}}{1 - x}\,.$$

So we would like to convert the sum above to look like the sum of a geometric sequence. To do that, we will use the fact that we have a primitive root g modulo p.

Note that, for g as above, we have

$$\{1, \cdots, p-1\} \mod p = \{g^0 = 1, g^1, \cdots, g^{p-2}\} \mod p\,.$$

Note then that

$$S_k \equiv g^{0\cdot k} + g^{1\cdot k} + \cdots + g^{(p-2)\cdot k} \mod p\,.$$

Using the identity above with $x = g^k$ and $m = p - 2$, we see that

$$(1 - g^k)S_k \equiv 1 - (g^k)^{p-1} \equiv 1 - (g^{p-1})^k \equiv 0 \mod p\,.$$

In other words,

$$p \text{ divides } (1 - g^k)S_k\,.$$

Case 1: $p-1$ does not divide k: In that case, $1 - g^k \not\equiv 0 \mod p$, since g is a primitive root modulo p. As a result, p does not divide $1 - g^k$. Since we saw above that

$$p \text{ divides } (1 - g^k)S_k\,,$$

it follows that, since p is a prime, p must divide S_k.

As a result, we checked that S_k is divisible by p whenever $p - 1 \nmid k$.

Case 2: $p-1$ divides k: In that case,

$$S_k = 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv \underbrace{1 + \cdots + 1}_{p-1 \text{ terms}}\ p - 1 \not\equiv 0 \mod p\,.$$

In other words, if $p - 1$ divides k, then S_k is not divisible by p.

Answer: All integers that are not divisible by $p - 1$.

3.2. **Quadratic Reciprocity Law (Gauss' "Golden Theorem").**

3.2.1. Suppose p is a prime number and a is an integer. We define the Legendre symbol $\left(\frac{a}{p}\right)$ on setting

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if } p \nmid a \notin \square_p\,, \\ +1 & \text{if } a \in \square_p\,, \\ 0 & \text{if } p \mid a. \end{cases}$$

3.2.2. *Legendre symbol is multiplicative.* We have

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

Indeed, if a or b is divisible by p, then both sides are equal to 0. Assume therefore that $p \nmid ab$.

Let g be a primitive root and let m, n be integers so that

$$g^m \equiv a\,, g^n \equiv b \mod p\,.$$

Then we would like to check that

$$\left(\frac{g^{m+n}}{p}\right) = \left(\frac{g^m}{p}\right)\left(\frac{g^n}{p}\right).$$

We have checked earlier that

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

namely that even powers of g are squares mod p, and odd powers are not. As a result,

$$\left(\frac{g^{m+n}}{p}\right) = (-1)^{m+n} = (-1)^m(-1)^n = \left(\frac{g^m}{p}\right)\left(\frac{g^n}{p}\right),$$

as desired.

This is somewhat surprising: It tells us that the product of two non-squares mod p is a square mod p.

3.2.3. *Quadratic Reciprocity Law.* Suppose that p and q are odd primes. Then:

i) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.
ii) $\left(\frac{2}{q}\right) = (-1)^{\frac{p^2-1}{8}}$.
iii) $\left(\frac{-1}{q}\right) = (-1)^{\frac{p-1}{2}}$.

We actually proved the very last property:

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

3.2.4. *Example.* Let us see if 101 is a square modulo 997. This amounts to calculating the Legendre symbol $\left(\frac{101}{997}\right)$. I dare you to decide whether or not there is an x such that $x^2 \equiv 101 \mod 997$ using brute force!

Gauss: $\left(\frac{101}{997}\right) = (-1)^{\frac{100\times 996}{4}}\left(\frac{997}{101}\right) = \left(\frac{997}{101}\right) = \left(\frac{-13}{101}\right)$ where the final equality is because $997 \equiv -13 \mod 101$. Hence,

$$\left(\frac{101}{997}\right) = \left(\frac{-13}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{13}{101}\right) = (-1)^{\frac{100}{2}}\left(\frac{13}{101}\right) = \left(\frac{13}{101}\right).$$

Gauss again: $\left(\frac{13}{101}\right) = (-1)^{\frac{12\times 100}{4}}\left(\frac{101}{13}\right) = \left(\frac{10}{13}\right)$, where the final equality is because $101 \equiv 10 \mod 13$. Hence,

$$\left(\frac{101}{997}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = (-1)^{\frac{168}{8}}\left(\frac{5}{13}\right) = -\left(\frac{5}{13}\right).$$

Here, the third equality uses QRL(ii).

Gauss once again: $\left(\frac{101}{997}\right) = -\left(\frac{5}{13}\right) = -(-1)^{\frac{4\times 12}{4}}\left(\frac{13}{5}\right) = -\left(\frac{3}{5}\right) = -1 \times -1 = 1$, where the penultimate equality is because the only squares modulo 5 are 1 and 4 (check by hand!).

That means 101 is indeed a square modulo 997. Amazing, isn't it?!

Kâzim Büyükboduk
UCD School of Mathematics and Statistics, University College Dublin, Ireland

Email address: kazim.buyukboduk@ucd.ie