

MATH 361: NUMBER THEORY — FOURTH LECTURE

1. INTRODUCTION

Everybody is familiar with *modular arithmetic*, meaning the usual arithmetic of the integers subject to the additional condition that some fixed integer (such as 12) is to be viewed as 0. Three hours after 10:00, the time is 1:00.

2. CONGRUENCE

Definition 2.1. For any integers a , b , and n , we say that **a equals b modulo n** , notated

$$a = b \pmod{n},$$

if $n \mid b - a$. Other notations for congruence are

$$a =_n b, \quad a \equiv b \pmod{n}, \quad a = b (n),$$

and so on.

Although there is nothing new in the definition other than notation, the notation emphasizes that the properties of congruence are similar to the properties of equality. The congruence notation lets us phrase arguments neatly and naturally. Here are some examples.

- $a = b \pmod{0}$ if and only if $a = b$.
- $a = b \pmod{1}$ for all a and b .
- $a = b \pmod{2}$ if and only if a and b have the same parity.
- An exercise on the first homework set showed that

$$f(n_o + kf(n_o)) = 0 \pmod{f(n_o)}.$$

- Let $f \in \mathbf{Z}[X_1, \dots, X_k]$ (a polynomial in k variables with integer coefficients) be given. Suppose that we have k pairs of integer values that are congruent modulo some n ,

$$x_1 = y_1 \pmod{n}, \quad \dots, \quad x_k = y_k \pmod{n}.$$

Then also

$$f(x_1, \dots, x_k) = f(y_1, \dots, y_k) \pmod{n}.$$

In particular,

$$\left\{ \begin{array}{l} x_1 = y_1 \pmod{n}, \\ x_2 = y_2 \pmod{n} \end{array} \right\} \implies \left\{ \begin{array}{l} x_1 + x_2 = y_1 + y_2 \pmod{n}, \\ x_1 x_2 = y_1 y_2 \pmod{n} \end{array} \right\}.$$

- (*Decimal digits*) Since $10 = 1 \pmod{9}$, it follows that for any decimal digits a_0, \dots, a_n ,

$$\sum_{i=0}^n a_i 10^i = \sum_{i=0}^n a_i \pmod{9}.$$

This is the grade school result that a number is divisible by 9 if and only if the sum of its digits is divisible by 9. Since $10 = -1 \pmod{11}$ a similar result holds for divisibility by 11, but with the alternating sum of the digits.

- (*A variant of Euclid's argument*) Any odd n satisfies $n = 1 \pmod{4}$ or $n = 3 \pmod{4}$. Suppose that there are only finitely primes $p = 3 \pmod{4}$; call them p_i for $i = 1, \dots, k$. (So here $p_1 = 3$.) Consider the odd number

$$n = 4p_2 \cdots p_k + 3 \quad (\text{note that } p_1 = 3 \text{ is excluded}).$$

Then $n \not\equiv 0 \pmod{3}$ and $n = 3 \pmod{p_i} \not\equiv 0 \pmod{p_i}$ for $i = 2, \dots, k$. Thus none of the p_i divide n , and neither does 2. It follows that n is a product of primes $q = 1 \pmod{4}$. But any such product is again $1 \pmod{4}$, contradicting the fact that $n = 3 \pmod{4}$. The conclusion is that there exist infinitely many primes $p = 3 \pmod{4}$.

3. EULER'S RULE AND FERMAT'S LITTLE THEOREM

Proposition 3.1 (Euler's Rule). *Let a, n be integers with $(a, n) = 1$. Then*

$$a^{\phi(n)} = 1 \pmod{n}.$$

Proof. For an elementary proof, let $x_1, \dots, x_{\phi(n)}$ be the elements of $\{0, \dots, n-1\}$ that are coprime to n . Then

$$ax_i = x_{j(i)} \pmod{n}, \quad i = 1, \dots, \phi(n),$$

where the map

$$i \longmapsto j(i)$$

permutes $\{1, \dots, \phi(n)\}$. (Here the point is that if $ax_i = ax_{i'}$ then $x_i = x_{i'}$ since a is coprime to n , and so $x_i = x_{i'}$ since both come from $\{0, \dots, n-1\}$, i.e., $i = i'$.) Since the map is a permutation, we have

$$\prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} (ax_i) = a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i.$$

It follows that $1 = a^{\phi(n)} \pmod{n}$ because $\prod_{i=1}^{\phi(n)} x_i$ is coprime to n . \square

In fact, Euler's Rule is a special case of a basic result of group theory. Working in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$, the powers of a generate a subgroup $\langle a \rangle$. The order of the subgroup divides the order of the group, and so raising a to some power $e \mid \phi(n)$ gives 1 in $(\mathbf{Z}/n\mathbf{Z})^\times$. Euler's Rule follows.

Corollary 3.2 (Fermat's Little Theorem). *Let a be a nonzero integer, and let $p \nmid a$ be prime. Then*

$$a^{p-1} = 1 \pmod{p}.$$

Consequently $a^p = a \pmod{p}$ for all integers a and primes p .

4. THE QUOTIENT RING $\mathbf{Z}/n\mathbf{Z}$

Let $n \in \mathbf{Z}^+$ be a positive integer. Congruence modulo n partitions \mathbf{Z} into the equivalence classes

$$\begin{aligned} \bar{0} &= 0 + n\mathbf{Z}, \\ \bar{1} &= 1 + n\mathbf{Z}, \\ &\vdots \\ \overline{n-1} &= (n-1) + n\mathbf{Z}. \end{aligned}$$

This collection of equivalence classes inherits a ring structure from \mathbf{Z} via the rules

$$\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a + b}, \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{ab}.$$

That is,

$$(a + n\mathbf{Z}) + (b + n\mathbf{Z}) \stackrel{\text{def}}{=} (a + b) + n\mathbf{Z}, \quad (a + n\mathbf{Z})(b + n\mathbf{Z}) \stackrel{\text{def}}{=} ab + n\mathbf{Z}.$$

Informally we are doing *remainder arithmetic*, but really a quotient entity such as $\bar{3}$ means *3 and all its n-translates*. The number of hours from *any* 10:00 to *any* 1:00 is $\bar{3}$ rather than 3.

The reduction map

$$\bar{} : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$$

is a ring homomorphism by definition, meaning that it preserves sums and products. What is in question is whether it is even sensible. The point is that possibly $\bar{a} = \bar{a'}$ and $\bar{b} = \bar{b'}$ in $\mathbf{Z}/n\mathbf{Z}$ even though $a \neq a'$ and/or $b \neq b'$ in \mathbf{Z} , and so the sum

$$\bar{a} + \bar{b} = \bar{a'} + \bar{b'}$$

is defined by two different formulas,

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a'} + \bar{b'} = \overline{a' + b'}.$$

So unless $\overline{a + b} = \overline{a' + b'}$, the reduction map is not sensible. However, we know that

$$a = a' \pmod{n} \quad \text{and} \quad b = b' \pmod{n},$$

so that

$$a + b = a' + b' \pmod{n}.$$

This is the desired result. Similarly, $ab = a'b' \pmod{n}$, showing that multiplication in the quotient $\mathbf{Z}/n\mathbf{Z}$ is well defined as well.

The unit group of $\mathbf{Z}/n\mathbf{Z}$ is

$$(\mathbf{Z}/n\mathbf{Z})^\times = \{a \in \mathbf{Z}/n\mathbf{Z} : ab = 1 \text{ for some } b \in \mathbf{Z}/n\mathbf{Z}\}$$

Our earlier discussion of ideals and the Euclidean algorithm shows that for any integer $a \in \mathbf{Z}$,

$$(a, n) = 1 \iff ab + kn = 1 \text{ for some } b, k \iff \bar{a} \in (\mathbf{Z}/n\mathbf{Z})^\times.$$

Consequently,

$$(\mathbf{Z}/n\mathbf{Z})^\times = \{\bar{a} : (a, n) = 1\}.$$

It follows by definition of the Euler totient function that

$$|(\mathbf{Z}/n\mathbf{Z})^\times| = \phi(n).$$

5. THE EQUATION $ax + ny = b$

We are assuming that $a, n, b \in \mathbf{Z}$ and $n \neq 0$. The equation in the section-header rewrites as

$$Av = b, \quad A = [a \quad n], \quad v = \begin{bmatrix} x \\ y \end{bmatrix}.$$

A solution $(x_o, y_o) \in \mathbf{Z}^2$ exists if and only if $(a, n) \mid b$. When such a solution exists then by linear algebra, the general solution in \mathbf{Q}^2 is then

$$(x, y) = (x_o, y_o) + \mathbf{Q}(-n, a),$$

and so the general solution in \mathbf{Z}^2 is

$$(x, y) = (x_o, y_o) + \mathbf{Z} \frac{(-n, a)}{(a, n)}.$$

(Note that in the previous display, the (a, n) in the denominator is a gcd, while all the other ordered pairs are vectors.) Especially, the x -coordinates of the solutions are

$$x = x_o + \mathbf{Z} \frac{n}{(a, n)}.$$

6. THE CONGRUENCE $ax = b \pmod n$

Again consider $a, b, n \in \mathbf{Z}$ with $n \neq 0$. For any $x \in \mathbf{Z}$ we have the equivalences

$$\begin{aligned} ax = b \pmod n &\iff n \mid ax - b \\ &\iff ax - b = ny \text{ for some } y \\ &\iff ax + ny = b \text{ for some } y. \end{aligned}$$

So the work that we just did shows the following result.

Proposition 6.1. *Let $a, b, n \in \mathbf{Z}$ with $n \neq 0$. The congruence*

$$ax = b \pmod n$$

has solutions if and only if $(a, n) \mid b$. When the congruence has a solution $x_o \in \mathbf{Z}$ then the full solution set is

$$\{x_o + tn/(a, n) : t \in \mathbf{Z}\}.$$

It follows that the equation $ax = b$ in $\mathbf{Z}/n\mathbf{Z}$ has (a, n) solutions. In particular, if $(a, n) = 1$ then the equation $ax = b$ has one solution in $\mathbf{Z}/n\mathbf{Z}$.

Perhaps the proposition is most easily remembered as follows:

Consider the congruence

$$ax = b \pmod n.$$

Let

$$g = \gcd(a, n), \quad a = a'g, \quad n = n'g.$$

Then the congruence is

$$a'gx = b \pmod{n'g}.$$

Unless $b = b'g$ there are no solutions. If $b = b'g$ then the congruence becomes

$$a'x = b' \pmod{n'}, \quad \gcd(a', n') = 1,$$

with solution

$$x = a'^{-1}b' \pmod{n'}.$$

Thus there are $n/n' = g$ solutions modulo n .