Congruences, The Chinese Remainder Theorem, The Euler "Phi-function"

September 13, 2012

1 New Reading and Homework due September 20:

1. Read Chapter 3 Sections 1,2 of **[I-R]**
2. Page 26, Exercises 3-7 item Page 27: Exercises 10,11.
3. Page 27: Exercise 15 (a), (b).
4. Page 27: Exercises 20,21,(*Correct 22*),
5. Enjoy this exercise: you need not hand it in Page 27: Exercise 27.

2 Congruence, and congruence classes

2.1 *Congruence notation:*

$$a \equiv b \text{ modulo } N$$

means equivalently:

- $a = b + mN$ for some integer m,
- $N \mid a - b$,
- $a + N\mathbf{Z} = b + N\mathbf{Z} \subset \mathbf{Z}$.
- *Vocabulary:* a and b are in the "same congruence class modulo N."

3 The ring $\mathbf{Z}/N\mathbf{Z}$

This is the ring of congruence classes of integers modulo the ideal generated by the positive number N. Its cardinality is N; its elements are cosets

$$\bar{0} := 0 + N\mathbf{Z},\ \bar{1} := 1 + N\mathbf{Z},\ \bar{2} := 2 + N\mathbf{Z},\ \ldots, \bar{(N-1)} := (N-1) + N\mathbf{Z}.$$

So, in this notation (which is bad, discuss) the (surjective) ring homomorphism $\mathbf{Z} \to \mathbf{Z}/N\mathbf{Z}$ sends $a \to \bar{a}$. The kernel of this homomorphism is $\bar{0} = N\mathbf{Z}$. Discuss other formats.

3.1 Arithmetic in the ring $\mathbf{Z}/N\mathbf{Z}$

Discuss examples. E.g., modulo $N = 10$. Polynomial equations. Finding square roots is hard.

4 Chinese Remainder Theorem

Discuss by examples. First, consider "forgetting information in congruence classes": if I have a congruence class modulo ab I can take any representative and consider it modulo a and I get a congruence class mod a; ditto for b. This gives a natural ring homomorphism $\mathbf{Z}/ab\mathbf{Z} \to \mathbf{Z}/a\mathbf{Z}$; ditto for b to get a ring homomorphism $\mathbf{Z}/ab\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$. Put them together to get a ring homomorphism

$$(*) \quad \mathbf{Z}/ab\mathbf{Z} \to \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}.$$

Give a few examples.

Theorem 1 (Chinese Remainder Theorem) *if a, b are relatively prime then the homomorphism above is an isomorphism of rings*

$$\mathbf{Z}/ab\mathbf{Z} \simeq \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}.$$

Basic idea of the proof: There are integers r, s such that $1 = ra + sb$. Note that

$$ra \equiv 1 \text{ mod b}$$

and

$$sb \equiv 1 \text{ mod a}.$$

For any pair of integers x and y representing congruence classes modulo b and modulo b respectively. Giving us a congruence class $(\bar{x})$ mod b and a congruence class $(\bar{y})$ mod a, consider this extraordinary concoction: the integer

$$xra + ysb.$$

Discuss!

The question to ask about this funny integer is: what is it modulo a? and what is it modulo b? Since $ra \equiv 1$ mod b we get that it is $x \cdot 1 + 0 = x$ modulo b and it is $0 + y \cdot 1$ modulo a. Note that the rule

$$(y, x) \mapsto xra + ysb$$

induces a ring homomorphism

$$(**) \quad \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \to \mathbf{Z}/ab\mathbf{Z}$$

that is a two-sided inverse to **(*)**,

In simpler terms:

> Given any congruence class modulo a and any congruence class modulo b there is a unique congruence class modulo ab that gives the first congruence class when reduced mod a and the second one when reduced mod b.

Corollary 2

$$\mathbf{Z}/\prod_p p^{e_p}\mathbf{Z} \simeq \prod_p \mathbf{Z}/p^{e_p}\mathbf{Z}.$$

5 The group of units in $\mathbf{Z}/N\mathbf{Z}$

Define and discuss groups of units in rings.

Notation: $(\mathbf{Z}/N\mathbf{Z})^*$ or, as the text has it, $U(\mathbf{Z}/N\mathbf{Z})$.

Proposition 1

$$(\mathbf{Z}/N\mathbf{Z})^* = \{\bar{a} \mid (a, N) = 1 \text{ and } 1 \leq a \ \leq N\}.$$

Proof: Any congruence class mod N is represented by a unique integer a in the range $[0, N-1]$. If such an a is relatively prime to N, we can write $1 = ra + sN$ for some r, s and reading this modulo N says that the congruence class mod N represented by r is the inverse to that represented by a. In other words, a is a unit mod N. Going the other way, (i.e., if the congruence class represented by a is a unit mod N, then a is relatively prime to N) is similar.

Corollary 3 *If a and b are relatively prime, then*

$$(\mathbf{Z}/ab\mathbf{Z})^* \simeq (\mathbf{Z}/a\mathbf{Z})^* \times (\mathbf{Z}/b\mathbf{Z})^*.$$

sectionThe Euler "Phi-function"

Definition 1 *Let $n > 0$. The Euler "Phi-function" $\Phi(n)$ is defined to be the number of integers $\leq n$ that are relatively prime to n.*

Corollary 4

$$|(\mathbf{Z}/N\mathbf{Z})^*| = \Phi(N).$$

Corollary 5 *$N \mapsto \Phi(N)$ is a multiplicative arithmetic function.*

Corollary 6 *If*

$$N = \prod_{p \text{ prime } \mid p \text{ divides } N} p^{e_p},$$

then

$$\Phi(N) = \prod_p (p-1) \cdot p^{e_p - 1}.$$

5.1 Arithmetic mod N

Discuss Linear equations: $AX + B \equiv C$ modulo N.

When can you solve, and when not?

5.2 Specifically about the field $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$

Corollary 7 *If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a field (called the prime field of characteristic p, and denoted $\mathbf{F}_p$).*

Corollary 8 *If p is a prime number and a is not divisible by p, then $a^{p-1} \equiv 1$ modulo p.*

Give alternate proof by induction. Discuss "raising to the p-th power" in $\mathbf{F}_p$.

The *Rabin a-test:* take a number P that you wish to test whether or not it is a prime and compute a^{P-1} modulo P. *If the answer isn't* 1*, then P is* **not** *a prime.* But, of course, if the answer is 1, you really know nothing. As a fun exercise you can try your hand at finding the smallest composite number that "passes" the 2-test, the 3-test.

For your information: One can show that 3452690329392158031464109281736967404068448156 84 $\sim$ 2396721012992064214519445919256941544565276067662360108749727241555708425276527278687 76 $\sim$ 3629595196208727356122006010365068716811246109865968781807389014865 27 is NOT a prime by the Rabin 2-test.