The Euler "Phi-function," Congruences mod p

September 18, 2012

1 Readings:

Read Chapter 3 and section 1 of Chapter 4.

2 The Euler "Phi-function"

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

Corollary 1

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

Corollary 2 *$N \mapsto \Phi(N)$ is a multiplicative arithmetic function.*

Corollary 3 *If*

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

then

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

3 Arithmetic mod N

3.1 *Linear equations*

$$(*)_N \qquad AX + B \ \equiv \ C \bmod \text{N}.$$

When can you solve, and when not?

If $N = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ then equation $(*)_N$ above is "equivalent to" a system of t equations:

$$(*)_{p_i^{e_i}} \qquad AX + B \equiv C \bmod \mathrm{p_i^{e_i}}.$$

Similarly for any polynomial equation modulo N.

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

Corollary 4 *If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a field (called the prime field of characteristic p, and denoted $\mathbf{F}_p$).*

In other words, equation

$$(*)_p \qquad AX + B \equiv C \bmod \mathrm{p}$$

has a solution if $A \not\equiv 0$ mod p and this solution is "unique" (i.e., the congruence class mod p represented by any solution is unique).

Question: Can you give necessary and sufficient conditions on the set of triples A, B, C such that there exists a "unique" solution to $(*)_N$.

4 Basic introduction to polynomial rings over fields

Revisit the Euclidean algorithm, the fundamental divisibility lemma, the unique factorization theorem. Intro to Gaussian integers.

Corollary 5 *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 $\mathbf{F}_p$.

5 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 345269032939215803146410928173696740406844815684 ∼ 23967210129920642145194459192569415445652760676623601087497272415557084252765272786877 6 ∼ 362959519620872735612200601036506871681124610986596878180738901486527 is NOT a prime by the Rabin 2-test.

Challenge: Find the first *non*-prime that fails the Rabin 2-test. The Rabin 3-test.
Challenge for Computers: Experiment with this phenomenon!

6 A bit of group theory and Euler's Theorem

Proposition 1 *If G is a finite group and $x \in G$, then the order of x divides the order of G*

Corollary 6 *If $(a, N) = 1$ then $a^{\Phi(N)} \equiv 1$ modulo N.*

Discuss extraction of square roots. Examples. $X^2 - 1 = (X - 1)(X + 1)$. ± 1 are the only two congruence classes that are *equal* to their own inverses.

Proposition 2 Wilson's theorem *Let p be prime. Then $(p-1)! \equiv -1$ modulo p*

Corollary 7 *Let p be a prime that is congruent to 1 mod 4. Then $(\frac{p-1}{2})!$ (modulo p) is a root of the polynomial $X^2 + 1$. That is, it represents a "square root of minus one" in the field $\mathbf{F}_p$.*

Corollary 8 *A rational prime p (i.e., an old-fashioned prime in the integers) remains prime in the ring of Gaussian integers if and only if it is congruent to -1 modulo 4.*

7 Quadratic equations

7.1 Quadratic polynomials in the field $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$

$$(**)_p \qquad AX^2 \ + \ BX \ + \ C \ \equiv \ 0 \text{ mod p.}$$

Discuss the "moral" of the quadratic formula: reduction to finding *square roots*. Except when $p = 2$.

Discuss quadratic residues.