The structure of $(\mathbf{Z}/p\mathbf{Z})^*$

September 25, 2012

1 Readings:

1. Read Wikipedia's entry on primitive roots.
2. Read sections 1,2 of Chapter 5 of [**I-R**].

2 Primitive root

We will keep to p a prime and work mod p. Recall the definition of primitive root.

Definition 1 *A* **primitive root** *mod p is a congruence class $\gamma \in \mathbf{F}_p^*$ that generates $\mathbf{F}_p^*$; i.e., it is a class γ such that*

$$\mathbf{F}_p^* = \{1 = \gamma^0, \gamma^1, \gamma^2, \ldots, \gamma^{p-2}\}.$$

Equivalently, it is a class in $\mathbf{F}_p^*$ of order $p-1$.

Proposition 1 *The number of primitive roots modulo p is equal to $\Phi(p-1)$.*

Proof: For any integer d let $\psi(d)$ denote the number of elements of $\mathbf{F}_p^*$ of order d. (So, $psi(d) = 0$ unless $d \mid p-1$.) We must show that

$$\psi(p-1) \stackrel{?}{=} \Phi(p-1).$$

1. **Step 1: Certain subgroups of $\mathbf{F}_p^*$**

   For any positive integer d, define:

   $$\mathbf{F}_p^*\langle d\rangle := \{u \in \mathbf{F}_p^* \mid u^d = 1\}.$$

   Caution: I refer to this as the set—it is actually a subgroup (prove this!)—of elements in $\mathbf{F}_p^*$ *killed by raising-to-the-d-th power*. These are not (only) the elements of *order* d in $\mathbf{F}_p^*$. Rather, these are all the elements of $\mathbf{F}_p^*$ of order any divisor of d.

   Proposition 2 *Let d be a divisor of $p-1$. The order of the subgroup $\mathbf{F}_p^*\langle d\rangle$ is d.*

   Proof: Since $d \mid p-1$, the polynomial $X^d - 1$ divides the polynomial $X^{p-1} - 1$ in the ring $\mathbf{F}_p[X]$. Now $X^{p-1} - 1$ factor into the product of $p-1$ distinct linear monic factors; therefore $X^d - 1$ factors similarly into d distinct linear factors; i.e.: QED.

   Corollary 1 *For any $d \mid p-1$ we have the formula:*

   $$(*) \qquad \sum_{c \mid d} \psi(c) = d.$$

   Proof: We have:

   $$\mathbf{F}_p^*\langle d\rangle \ = \sqcup_{c \mid d}\{\text{elements of order } c \text{ in } \mathbf{F}_p^*\langle d\rangle.$$

   But if $c \mid d$ then any element of order c is contained in $\mathbf{F}_p^*\langle d\rangle$. QED

2. **Step 2: Getting the same formula for $\Phi(d)$**

   $$(**) \qquad \sum_{c \mid d} \Phi(c) = d.$$

   Proof: Reduce to lowest terms the following d fractions:

   $$\frac{1}{d}, \frac{2}{d}, \frac{3}{d}, \ldots, \frac{d}{d}.$$

   For any c dividing d, exactly $\Phi(c)$ of these reduced-to-lowest-terms fractions will have denominator c. QED

3. **Step 3: Concluding, e.g., by Moebius inversion**

Corollary 2 *Any prime p has a primitive root. The group $\mathbf{F}_p^*$ is cyclic of order $p-1$. The subgroup $\mathbf{F}_p^*\langle d\rangle$ for d a divisor of $p-1$ is the unique subgroup of $\mathbf{F}_p^*$ of order d; and is cyclic.*

1. Fix a primitive root, g. We have a neat way of expressing all congruence classes (except 0) mod p as powers of g. Define **index** (relative to g—a logarithm of sorts).

2. If $p \neq 3$ the product of its primitive roots is congruent to 1 (mod p). Why?

3. The sum of all primitive roots is congruent to $\mu(p-1)$ (mod p).

4. *The size of g_p, the smallest primitive root mod p:*

   (a) For infinitely many p, $g_p >> \log p$.

   (b) The going guess: there are constants C and n such that $g_p \leq C \log^n(p)$. Given GRH, (Discuss) it is proved that one can take $n = 6$.

5. *For how many primes p is a given number a a primitive root?*

   (a) Let a be square-free. Denote by $\Sigma(a)$ the set of prime numbers p such that a is a primitive root modulo p. Then *Artin Conjectured* that $\Sigma(a)$ has a *positive asymptotic density* inside the set of all primes. (Discuss) In particular, if this conjecture is true, $\Sigma(a)$ would be infinite. If a is not congruent to 1 mod 4, this density is *independent of* a and equals a number called *Artin's constant*:

$$C_{\text{Artin}} = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) = 0.3739558136\ldots.$$

3 The Legendre symbol

Recall:

Definition 2 *Let p be an odd prime and $a \in Z$. Then:*

$$\left(\frac{a}{p}\right) \in \{0, \pm 1\}$$

is the value 0 if $a \equiv 0$ modulo p; it is $+1$ if there exists a b such that $a \equiv b^2$ modulo p; and it is -1 if none of the above.

We have:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p.$$

Recall the corollary to Wilson's Theorem:

Corollary 3 *Let $p \equiv 1$ modulo 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 $\mathbf{F}_p$.*

Proposition 3

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