2. Congruences

Recall that $x \equiv a \pmod{m}$ means that $m \mid (x-a)$, or that $x = a + km$ for some $k \in \mathbb{Z}$. Recall too that if $a, b \in \mathbb{Z}$ then there are $a', b' \in \mathbb{Z}$ such that $aa' + bb' = \gcd(a, b)$. The numbers a', b' can be found using the Extended Euclidean Algorithm, which you may recall from your First Year. In particular, when $\gcd(a, b) = 1$ there are $a', b' \in \mathbb{Z}$ such that $aa' + bb' = 1$. Then $aa' \equiv 1 \pmod{b}$, so that a' is the inverse of $a \pmod{b}$.

2.1. **Chinese Remainder Theorem.**

Theorem 2.1 (Chinese Remainder Theorem)**.** *Given $m_1, \ldots, m_k \in \mathbb{N}$ with $\gcd(m_i, m_j) = 1 \quad (i \neq j)$ ("pairwise coprime"), and $a_1, \ldots, a_k \in \mathbb{Z}$, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a solution $x \in \mathbb{Z}$.

Proof. In fact x can be constructed explicitly. For $i = 1, \ldots, k$ define m_i' to be the inverse $\pmod{m_i}$ of $m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$, so that

$$m_1 \ldots m_{i-1} m_i' m_{i+1} \ldots m_k \equiv 1 \pmod{m_i}.$$

Then $x = \sum_{i=1}^{k} a_i m_1 \ldots m_{i-1} m_i' m_{i+1} \ldots m_k \equiv a_i \pmod{m_i}$ for $i = 1, \ldots, k$, because every term except the ith is divisible by m_i. □

Then, if x_0 is one solution to this set of congruences, it's easy to see (how?) that the general solution is $x = x_0 + \ell m_1 \cdots m_k$ for any integer ℓ. In particular, there is always a choice of ℓ giving a unique solution x in the range $0 \leq x < m_1 \cdots m_k$ of the set of congruences.

Q. If the m_i not pairwise coprime, what is the condition on the a_i's so that the set of congruences above again has a solution x?

One answer: factorize each m_i as a product of prime powers:

$$m_i = \prod_j p_j^{r_{ji}},$$

where the p_j's are the prime factors of $\prod_i m_i$, and the r_{ji} are all ≥ 0. Then replace the congruence $x \equiv a_i \pmod{m_i}$ by the set of congruences $x \equiv a_i \pmod{p_j^{r_{ji}}}$ for each j (justify!). Next, collect together all the congruences whose modulus is a power of the same prime, say (changing notation!) $x \equiv a_1 \pmod{p^{n_1}}, \ldots, x \equiv a_\ell \pmod{p^{n_\ell}}$. Then if these congruences are pairwise consistent, we need only take the one with the largest modulus (p^{n_ℓ} say). So we end up taking just one congruence for each p, and so the moduli we take are all pairwise coprime. (Two congruences $x \equiv a_1 \pmod{p^m}$ and $x \equiv a_2 \pmod{p^n}$ with $m \leq n$ (note: same p in both) are *pairwise consistent* if $a_2 \equiv a_1 \pmod{p^m}$.) If some

such pair of congruences are not consistent, then that pair of congruences, and hence the original set of congruences, has no solution.

An example of an inconsistent pair of congruences is $x \equiv 0 \pmod 2$, $x \equiv 1 \pmod 4$.

Lemma 2.2. (i) *The congruence* $ax \equiv b \pmod m$ *has a solution* $x \in \mathbb{Z}$ *if and only if* $\gcd(a,m) \mid b$*; in this case the number of solutions* x *is* $\gcd(a,m)$.

(ii) *If* $x^a \equiv 1 \pmod m$ *and* $x^b \equiv 1 \pmod m$ *then* $x^{\gcd(a,b)} \equiv 1 \pmod m$.

Proof. (i) Put $g = \gcd(a,m)$. Then $b = ax + km$ shows that $g \mid b$. Conversely, if $g \mid b$ then $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$ and $\gcd(\frac{a}{g}, \frac{m}{g}) = 1$ (justify!). So $\frac{a}{g}$ has an inverse $\pmod{\frac{m}{g}}$ and $x \equiv \frac{b}{g} \cdot \left(\frac{a}{g}\right)^{-1} \pmod{\frac{m}{g}}$.

The g different solutions to $ax \equiv b \pmod m$ are then $x_0 + k\frac{m}{g}$ for $k = 0, 1, \ldots, g-1$, for any solution x_0 of $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$.

(ii) We have $\gcd(a,b) = aa' + bb'$ say, by the Extended Euclidean algorithm, so

$$x^{\gcd(a,b)} = x^{aa'+bb'} = (x^a)^{a'} \cdot (x^b)^{b'} \equiv 1 \pmod m.$$

□

2.2. **Solving equations in $\mathbb{F}_p$.** We now restrict our congruences to a prime modulus p, and consider the solutions of equations $f(x) = 0$ for $f(x) \in \mathbb{F}_p[x]$ and $x \in \mathbb{F}_p$. Since $\mathbb{F}_p = \mathbb{Z}/(p)$, this is equivalent, for $f(x) \in \mathbb{Z}[x]$, of solving $f(x) \equiv 0 \pmod p$ for $x \in \{0, 1, 2, \ldots, p-1\}$.

Theorem 2.3. *A nonzero polynomial* $f \in \mathbb{F}_p[x]$ *of degree* n *has at most* n *roots* x *in* $\mathbb{F}_p$.

Proof. Use induction: for $n = 1$, $f(x) = ax + b$ say, with $a \neq 0$, whence $f(x) = 0$ has a solution $x = a^{-1}b$ in $\mathbb{F}_p$.

Now assume $n \geq 1$ and that the result holds for n. Take $f(x) \in \mathbb{F}_p[x]$ of degree $n+1$. If $f = 0$ has no roots $x \in \mathbb{F}_p$ the the result is certainly true. Otherwise, suppose $f(b) = 0$ for some $b \in \mathbb{F}_p$. Now divide $x - b$ into $f(x)$, (i.e., one step of the Euclidean algorithm for polynomials) to get $f(x) = (x-b)f_1(x) + r$ say, where f_1 is of degree n, and $r \in \mathbb{F}_p$. Putting $x = b$ shows that $r = 0$. Hence $f(x) = (x-b)f_1(x)$, where f_1 has, by the induction hypothesis, at most n roots $x \in \mathbb{F}_p$. So f has at most $n+1$ roots $x \in \mathbb{F}_p$, namely b and those of $f_1 = 0$. Hence the result is true for $n+1$ and so, by induction, true for all $n \geq 1$. □

Note that the proof, and hence the result, holds equally well when $\mathbb{F}_p$ is replaced by *any* field F. However, it does not hold when the coefficients of f lie in a ring with zero divisors. For instance, on replacing F by the ring $\mathbb{Z}/8\mathbb{Z}$, the equation $x^2 - 1 \equiv 0 \pmod 8$ has *four* solutions $x = 1, 3, 5, 7 \pmod 8$.

Question. Where in the above proof was the fact that we were working over a field used?

2.3. **$\mathbb{F}_p^\times$ is cyclic!** Denote by $\mathbb{F}_p^\times$ the multiplicative group $\mathbb{F}_p \setminus \{0\}$, using the field multiplication (and forgetting about its addition).

We need some group theory at this stage. Recall that the *exponent* of a finite group G is the least $e \in \mathbb{N}$ such that $g^e = 1$ for each $g \in G$.

Let C_r denote the cyclic group with r elements: $C_r = \{1, g, g^2, \ldots, g^{r-1} \mid g^r = 1\}$. Here

Proposition 2.4. *Let G be a finite abelian group with $\#G$ elements. If G is noncyclic then its exponent is $< \#G$.*

Proof. For the proof, recall the Fundamental Theorem of Abelian Groups, which tells us that any such G is isomorphic to a product

$$C_{n_1} \times C_{n_2} \times C_{n_3} \times \cdots \times C_{n_{k-1}} \times C_{n_k}$$

of cyclic groups, for some $k \in \mathbb{N}$ and integers $n_1, \ldots, n_k$ all > 1 and such that $n_1 \mid n_2$, $n_2 \mid n_3$, $\ldots, n_{k-1} \mid n_k$. Hence all n_i's divide n_k and so n_k is the exponent of G. However, $\#G = n_1 n_2 \ldots n_k$, which is greater than n_k as $k > 1$. □

Proposition 2.5. *For p an odd prime, the group $\mathbb{F}_p^\times$ is cyclic (of size $p-1$ of course).*

Proof. Suppose $\mathbb{F}_p^\times$ were noncyclic. Then, by the previous Proposition, there would exist an exponent $e < p-1$ such that $x^e = 1$ for each $x \in \mathbb{F}_p^\times$. But then the equation $x^e = 1$ would have more than e solutions in $\mathbb{F}_p$, contradicting Theorem 2.3. □

A generator g of the cyclic group $\mathbb{F}_p^\times$ (p an odd prime) is called a *primitive root* $\pmod p$. Then we can write $\mathbb{F}_p^\times = \langle g \rangle$.

2.4. **Number of primitive roots.** Given a prime p, how many possible choices are there for a generator g of $\mathbb{F}_p^\times$? To answer this, we need to define Euler's φ-function. Given a positive integer n, $\varphi(n)$ is defined as the cardinality of the set $\{k : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}$.

So for instance $\varphi(1) = 1$, $\varphi(6) = 2$ and $\varphi(p) = p - 1$ for p prime.

Proposition 2.6. *For p an odd prime, there are $\varphi(p-1)$ primitive roots* $\pmod p$.

Proof. Take one primitive root g. Then g^k is again a primitive root iff $(g^k)^\ell = g$ in $\mathbb{F}_p^\times$ for some ℓ, i.e., $g^{k\ell - 1} = 1$. But $g^n = 1$ iff $(p-1) \mid n$. So g^k is a primitive root iff $k\ell - 1 \equiv 0 \pmod{p-1}$. This is impossible (why?) if $\gcd(k, p-1) > 1$, while if $\gcd(k, p-1) = 1$ then the extended Euclidean algorithm will give us ℓ. □

2.5. **Quadratic residues and nonresidues.** Take p an odd prime, and $r \in \mathbb{F}_p^\times$. If the equation $x^2 = r$ has a solution $x \in \mathbb{F}_p^\times$ then r is called a *quadratic residue* $\pmod p$. If there is no such solution x, then r is called a *quadratic nonresidue* $\pmod p$.

Proposition 2.7. *Take p an odd prime, and g a primitive root* $\pmod p$. *Then the quadratic residues* $\pmod p$ *are the even powers of g, while the quadratic nonresidues* $\pmod p$ *are the odd powers of g. (So there are $\frac{p-1}{2}$ of each.)*

Proof. Suppose $r \in \mathbb{F}_p^\times$, with $r = g^k$ say. If k is even then $r = (g^{k/2})^2$, so that r is a quadratic residue $\pmod p$. Conversely, if $x = g^\ell$, $x^2 = r$, then $g^{2\ell - k} = 1$, so that $2\ell - k$ is a multiple of $p-1$, which is even. So k is even. □

2.6. **The Legendre symbol.** Let p be an odd prime, and $r \in \mathbb{F}_p^\times$. Then the *Legendre symbol* is defined as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 \text{ if } r \text{ is a quadratic residue;} \\ -1 \text{ if } r \text{ is a quadratic nonresidue.} \end{cases}$$

Note that, on putting $r = g^k$ we see that

$$\left(\frac{g^k}{p}\right) = (-1)^k = \begin{cases} 1 \text{ if } k \text{ is even;} \\ -1 \text{ if } k \text{ is odd.} \end{cases}$$

Next, recall Fermat's Theorem: that $r^{p-1} = 1$ for all $r \in \mathbb{F}_p^\times$. This is simply a consequence of $\mathbb{F}_p^\times$ being a group of size (order) $p-1$. (We know that $g^{\#G} = 1$ for each g in a finite group G.)

Proposition 2.8 (Euler's Criterion)**.** *For p an odd prime and $r \in \mathbb{F}_p^\times$ we have in $\mathbb{F}_p^\times$ that*

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

Proof. If $r = g^k$ then for k even

$$r^{\frac{p-1}{2}} = g^{k\frac{p-1}{2}} = (g^{p-1})^{k/2} = 1^{k/2} = 1,$$

while if k is odd, $k\frac{p-1}{2}$ is not a multiple of $p-1$, so $r^{\frac{p-1}{2}} \neq 1$. However, $r^{p-1} = 1$ by Fermat, so $r^{\frac{p-1}{2}} = \pm 1$ and hence $r^{\frac{p-1}{2}} = -1$. So, by Proposition 2.7, we have (1), as required. □

2.7. **Taking nth roots in $\mathbb{F}_p^\times$.** Take an odd prime p and g a fixed primitive root $\pmod p$. Then for any $B \in \mathbb{F}_p^\times$ we define the *index* (old-fashioned word) or *discrete logarithm* (current jargon) of B, written $\operatorname{ind} B$ or $\log_p B$, as the integer $b \in \{0, 1, \ldots, p-2\}$ such that $B = g^b$ in $\mathbb{F}_p$. Clearly the function $\log_p$ depends not only on p but also on the choice of the primitive root g.

Proposition 2.9. *Given $n \in \mathbb{N}$ and $B \in \mathbb{F}_p^\times$, the equation $X^n = B$ in $\mathbb{F}_p^\times$ has a solution $X \in \mathbb{F}_p^\times$ iff $\gcd(n, p-1) \mid \log_p B$.*

When $\gcd(n, p-1) \mid \log_p B$ then the number of distinct solutions X of $X^n = B$ in $\mathbb{F}_p^\times$ is $\gcd(n, p-1)$.

Proof. Write $B = g^b$, $X = g^x$, so that $g^{nx} = g^b$, giving $nx \equiv b \pmod{p-1}$. Now apply Lemma 2.2(i) to this congruence. □

For large primes p, the problem of finding the discrete logarithm $\log_p B$ of B appears to be an intractable problem, called the *Discrete Logarithm Problem*. Many techniques in Cryptography depend on this supposed fact. See e.g.,

http://en.wikipedia.org/wiki/Discrete_logarithm