Lecture 7

Congruences mod Primes, Order, Primitive Roots

Continuation of Proof of Hensel's Lemma. By lemma,

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$$

Now we want to have the right hand side $\equiv 0$ mod p^{j+1}.

$$f(a) + tp^j f'(a) \equiv 0 \mod p^{j+1} \leftrightarrow tf'(a) + \frac{f(a)}{p^j} \equiv 0 \mod p$$

this has a unique solution

$$t \equiv -\left(\frac{f(a)}{p^j}\frac{1}{f'(a)}\right) \mod p$$

■

Direct formula - start with solution a of $f(x) \equiv 0$ mod p, and we want a solution mod p^*. Set $a_1 = a$.

$$a_{j+1} = a_j - f(a_j)\overline{f'(a)} \pmod{p^{j+1}}$$

where $\overline{f'(a)}$ is an integer chosen once at the beginning of the algorithm, which only matters mod p. It's chosen such that $\overline{f'(a)}f'(a) \equiv 1$ mod p. Then $f(a_j) \equiv 0$ mod p^j for $j \geq 1$ as long as $f'(a) \not\equiv 0$ mod p.

Eg. Solve the congruence $x^2 \equiv -1 \mod 125$. ($f(x) = x^2 + 1$, $f'(x) = 2x$). Mod 5: $2^2 \equiv -1 \mod 5$, so set $a = 2$. $f'(a) \equiv 4$ mod 5, so can choose $\overline{f'(a)} = -1$.

$$\begin{aligned}
a_1 &= 2 \pmod 5 \\
a_2 &= a_1 - f(a_1)\overline{f'(a)} \pmod{25} \\
&= 2 - (5)(-1) \pmod{25} \\
&= 7 \pmod{25} \\
a_3 &= a_2 - f(a_2)\overline{f'(a)} \pmod{125} \\
&= 7 - (50)(-1) \pmod{125} \\
&= 57 \pmod{125}
\end{aligned}$$

Congruences to prime modulus: Assume that all the coefficients of $f(x) = a_n x^n + a_{n-1}x^{n-1} \cdots + a_0$ are reduced mod p and also that $a_n \not\equiv 0$ mod p. By dividing out by a_n, can assume that $f(x)$ is monic (ie., highest coefficient is 1). We can also assume degree n of f is less than p. If not, can divide f by $x^p - x$ to get

$$\begin{aligned}
f(x) &= g(x)(x^p - x) + r(x) \text{ with } \deg(r(x)) < p \\
f(a) &= g(a)(a^p - a) + r(a) \equiv r(a) \mod p \text{ by Fermat}
\end{aligned}$$

so roots of $f(x)$ mod p are the same as the roots of $r(x)$ mod p.

Theorem 28. *A congruence $f(x) \equiv 0$ mod p of degree n has at most n solutions.*

Proof. (imitates proof that polynomial of degree n has at most n complex roots)

Induction on n: congruences of degree 0 and 1 have 0 and 1 solutions, trivially. Assume that it holds for degrees $< n$ ($n \geq 2$)

If it has no roots, then we're done. Otherwise, suppose it does have a root α. Dividing $f(x)$ by $x - \alpha$, we get $g(x) \in \mathbb{Z}[x]$ and a constant r such that $f(x) = g(x)(x - \alpha) + r$. Now if we plug in α we get $f(\alpha) = (\alpha - \alpha)g(\alpha) + r = r$, which means that $f(\alpha) = r$ and $f(x) = (x - \alpha)g(\alpha) + f(\alpha)$.

We know that $f(\alpha) \equiv 0$ mod p. If β is any other root of $f(x)$ then we plug β into the equation to get $f(\beta) = (\beta - \alpha)g(\beta) + f(\alpha)$. Mod p, $f(\beta) \equiv (\beta - \alpha)g(\beta)$ mod p, so $0 \equiv (\beta - \alpha)g(\beta)$. We also assume that $\beta \not\equiv \alpha$, so $g(\beta) \equiv 0$ mod p.

So β is a root of $g(x)$ as a solution of $g(x) \equiv 0$ mod p. We know that $g(x)$ has degree $n - 1$, so by induction hypothesis $g(x) \equiv 0$ mod p has at most $n - 1$ solutions, which by including α gives $f(x)$ at most n solutions. ∎

Corollary 29. *If $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0$ mod p has more than n solutions, then all $a_i \equiv 0$ mod p.*

Theorem 30. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $f(x) \equiv 0$ mod p has exactly n distinct solutions if and only if $f(x)$ divides $x^p - p$ mod p. Ie., there exists $g(x) \in \mathbb{Z}[x]$ such that $f(x)g(x) = x^p - x$ mod p as polynomials (all coefficients mod p)*

Proof. Suppose $f(x)$ has n solutions. Then $n \leq p$ because only p possible roots mod p (ie., $\deg(f) \leq \deg(x^p - x)$). Divide $x^p - x$ by $f(x)$ to get

$$x^p - x = f(x)g(x) + r(x), \quad \deg(r) < \deg(f) = n$$

Now note, if α is a root of $f(x)$ mod p then plug in to get

$$\begin{aligned} \alpha^p - \alpha &= f(\alpha)g(\alpha) + r(\alpha) \\ &\equiv 0g(\alpha) + r(\alpha) \\ &\equiv r(\alpha) \mod p \end{aligned}$$

so α must be a solution to $r(x) \equiv 0$ mod p. Since $f(x)$ has distinct roots, we see that $r(x) \equiv 0$ mod p has n distinct solutions. But $\deg(r) < n$. So by corollary we must have $r(x) \equiv 0$ mod p as a polynomial (each coefficient is 0 mod p.) Ie., $x^p - p = f(x)g(x)$ mod p, and so $f(x)$ divides $x^p - x$.

Now suppose $f(x) | x^p - x$ mod p. Write $x^p - x \equiv f(x)g(x)$ mod p, where $f(x)$ is a monic of degree n and $g(x)$ is a monic of degree $p - n$. We want to show that $f(x)$ has n distinct solutions.

By previous theorem, $g(x)$ has at most $p - n$ roots mod p. If $\alpha \in 0, 1, \dots p - 1$ is not a root of $g(x)$ mod p then $\alpha^p - \alpha \equiv f(\alpha)g(\alpha)$ mod p, which by Fermat $\equiv 0$. Since $g(\alpha) \not\equiv 0$ mod p, $f(\alpha) \equiv 0$ mod p. So since there are at least $p - (p - n)$ such α, we see that $f(x)$ has at least n distinct roots mod p. By the theorem, $f(x)$ has at most n roots mod $p \Rightarrow f(x)$ has exactly n distinct roots mod p. ■

Corollary 31. *If $d|p-1$ then $x^d \equiv 1$ mod p has exactly d distinct solutions mod p.*

Proof. $d|p-1$, so $x^{d-1} - 1|x^{p-1} - 1$ as polynomials. $p - 1 = kd$, so $x^{kd} - 1 = (x^d - 1)(x^{(k-1)d} \cdots + 1)$. So $x^d - 1|x(x^{p-1} - 1) = x^p - x$. So has d solutions. ■

Corollary 32. *Another proof of Wilson's Theorem*

Proof. Let p be an odd prime. Let $f(x) = x(x-1)(x-2)\dots(x-p+1)$. This has $\deg p$ and p solutions mod p, so it must divide $x^p - x$ mod p. Both polynomials are monic of the same degree (p), so must be equal mod p.

$$x(x-1)\dots(x-(p-1)) \equiv x^p - x \mod p$$

Coefficient of x on the LHS is just $(-1)(-2)\dots(-(p-1)) = (-1)^{p-1}(p-1)! = (p-1)!$ since p is odd, and so $(p-1)! \equiv -1$ mod p (coefficient on RHS). ■

This tells us much more as well - eg., $1 + 2 + \cdots + p - 1 \equiv 0$ mod p for $p \geq 3$, and $(1)(2) + (1)(3) + \dots (2)(3) \cdots + (p-1)(p-2) \equiv 0$ mod p for $p \geq 5$.

If we have a product $f(x) = (x - \alpha_1)\dots(x - \alpha_n)$ then $f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \dots (-1)^n \sigma_n$. σ_i are elementary symmetric polynomials.

$$\begin{aligned}
\sigma_1 &= \sum \alpha_i \\
\sigma_2 &= \sum_{i<j} \alpha_i \alpha_j \\
\sigma_k &= \sum (\text{all products of } k \text{ roots } \alpha_i)
\end{aligned}$$

Question - We know by Euler that if $(n, 35) = 1$, then $n^{\phi(35)} = n^{24} \equiv 1$ mod 35. Can 24 be replaced by something smaller? Ie., what's the smallest positive integer N such that if $(n, 35) = 1$ then $n^N \equiv 1$ mod 35.

(Definition) Order: If $(a, m) = 1$ and h is the smallest positive integer such that $a^h \equiv 1$ mod m then say h is the **order** of a mod m. Written as $h = \text{ord}_m(a)$.

Lemma 33. *Let $h = \text{ord}_m(a)$. The set of integers k such that $a^k \equiv 1$ mod m is exactly the set of multiples of h.*

Proof. $a^{rh} \equiv (a^h)^r \equiv 1^r \equiv 1 \bmod m$. Suppose we have k such that $a^k \equiv 1 \bmod m$. Want to show $h|k$. Write $k = hq + r$ where $0 \leq r < h$. $1 \equiv a^k = a^{hq+r} = a^{hq}a^r \equiv 1a^r \equiv a^r \bmod m$, so $a^r \equiv 1 \bmod m$. But $r < h$. So if $r > 0$, contradicts minimality of h, which means that $r = 0$, and k is multiple of h. ■

Lemma 34. *If $h = \operatorname{ord}_m(a)$ then a^k has order $\frac{k}{(k,h)}$ mod m.*

Proof.

$$\begin{aligned} a^{kj} &\equiv 1 \mod m \\ &\leftrightarrow h|kj \\ &\leftrightarrow \frac{h}{(h,k)} | \frac{k}{(h,k)} j \\ &\leftrightarrow \frac{h}{(h,k)} | j \end{aligned}$$

So smallest such positive $j = \frac{h}{(h,k)}$. ■

Lemma 35. *If a has order h mod m and b has order k mod m, and $(h,k) = 1$, then ab has order hk mod m.*

Proof. We know

$$\begin{aligned} (ab)^{hk} &\equiv (a^h)^k (b^k)^h \\ &\equiv 1^k 1^h \\ &\equiv 1 \mod m \end{aligned}$$

Conversely suppose that $r = \operatorname{ord}_m(ab)$.

$$\begin{aligned} (ab)^r &\equiv 1 \mod m \\ (ab)^{rh} &\equiv 1 \mod m \\ (a^h)^r b^{rh} &\equiv 1 \mod m \\ b^{rh} &\equiv 1 \mod m \end{aligned}$$

so $k|rh \Rightarrow k|r$ (since $(k,h) = 1$), and similarly $h|r$. So $hk|r$, and so $hk = \operatorname{ord}_m(ab)$. ■

(Definition) Primitive Root: If a has order $\phi(m)$ mod m, we say that a is a **primitive root** mod m.

Eg. mod 7:

1	has order	1		
2	has order	3		($2^3 \equiv 1$ mod 7)
3	has order	6	✓	($\phi(7) = 6$)
4	has order	3		
5	has order	6	✓	($\phi(7) = 6$)
6	has order	2		

Lemma 36. *Let p be prime and suppose $q^e || p-1$ for some other prime q. Then there's an element mod p of order q^e.*

Assuming Lemma...

$$p - 1 = q_1^{e_1} q_2^{e_2} \ldots q_r^{e_r}$$

Lemma says that $\exists\, g_1$ with $\mathrm{ord}_p(g_1) = q_1^{e_1}$, g_2 with $\mathrm{ord}_p(g_2) = q_2^{e_2}$, etc. Set $g = g_1 g_2 \ldots g_r$. So by previous lemma above, g has order $q_1^{e_1} q_2^{e_2} \ldots q_r^{e_r} = p - 1$ because all q_i are coprime in pairs. $p - 1 = \phi(p)$, so g is a primitive root mod p.

Proof. Consider solutions of $x^{q^e} \equiv 1$ mod p. Because $q^e | p - 1$, $x^{q^e} - 1$ has exactly q^e roots mod p. If α is any such root, then $\mathrm{ord}_p(\alpha)$ must divide q^e.

So if it's not equal to q^e, it must divide q^{e-1}. Then α would have to be root of $x^{q^{e-1}} - 1 \equiv 0$ mod p, which has exactly q^{e-1} solutions. Since $q^e - q^{e-1} > 0$, there exists α such that $\mathrm{ord}_p(\alpha) = q^e$. ■