Recall

- Lagrange
- Fermat: $a^{p-1} \equiv 1 \pmod{p}$ for $(a,p)=1$

  $a^p \equiv a \pmod{p}$ for all a

- Wilson
- "n passes base a test" if $a^n \equiv a \pmod{n}$
- passing base 2 test : pseudoprime.

e.g. $n = 341$ is a pseudoprime.

$\overset{\overset{11\cdot 31}{\shortparallel}}{341}$ passes base 2 test. What about base 3 test?

- $3^{341} \equiv (\underbrace{3^{10}}_{1})^{34} \cdot 3 \equiv 3 \pmod{11}$

$3^8 \equiv 144 \equiv 20 \equiv -11$

$3^4 \equiv 9^2 \equiv 19 \equiv -12$

- $3^{341} \equiv (\underbrace{3^{30}}_{1})^{11} \cdot 3^{11} \equiv 3^{11} \equiv 3^1 \cdot 3^2 \cdot 3^8 \equiv 3 \cdot 9 \cdot (-11) \equiv 13 \pmod{31}$

$\Rightarrow 3^{341} \not\equiv 3 \pmod{341}$

$\Rightarrow 341$ fails base 3 test.

<u>Question:</u> Is there any composite number which passes base a test, i.e. $a^n \equiv a \pmod n$ for all a?

<u>Answer:</u> Yes, and they are called Carmichael numbers.

<u>Example:</u> $\underset{\overset{\shortparallel}{3\cdot 11\cdot 17}}{561}$ is a Carmichael number

- $a^{561} \equiv (a^2)^{280} \cdot a \equiv a \pmod 3$ when $(a,3)=1$,
  $a^{561} \equiv 0 \equiv a \pmod 3$ if $(a,3)\neq 1$.
- $a^{561} \equiv (a^{10})^{56} \cdot a \equiv a \pmod{11}$ when $(a,11)=1$.
  $a^{561} \equiv 0 \equiv a \pmod{11}$ if $(a,11)\neq 1$.
- mod 17 is similar: $a^{561} = (a^{16})^{35} \cdot a$.

$\Rightarrow a^{561} \equiv a \pmod{561}$ by CRT.

<u>Exercise:</u> Suppose $n = p_1 p_2 \cdots p_k$ is a product of distinct primes such that $p_i - 1 \mid n-1$ for $i = 1, 2, \ldots, k$, then n is a Carmichael number.

- Same idea with the example. The converse is also true, but we'll not prove now.

Congruences modulo p^k

We now focus on $f(x) \equiv 0 \pmod{p^k}$ ← polynomial

We can solve $f(x) \equiv 0 \pmod{p}$, using the solution we'll find we can next solve $f(x) \equiv 0 \pmod{p^2}$, and then $f(x) \equiv 0 \pmod{p^3}$, ... until mod p^k.

Example: $x^3 - x^2 - x + 4 \equiv 0 \pmod{27}$

Step 1: $x^3 - x^2 - x + 4 \equiv 0 \pmod{3}$

$\Rightarrow x \equiv 1, 2 \pmod{3}$

$\Rightarrow x = 3k+1$ or $x = 3k+2$

Step 2.1: $x = 3k+1$

$(3k+1)^3 - (3k+1)^2 - (3k+1) + 4 \equiv 0 \pmod{9}$

$\Rightarrow \cancel{27k^3} + \cancel{27k^2} + \cancel{9k} + 1 - \cancel{9k^2} - 6k - 1 - 3k - 1 + 4 \equiv 0 \pmod{9}$

$\Rightarrow \cancel{-9k} + 3 \equiv 0 \pmod{9}$

$\Rightarrow 3 \equiv 0 \pmod{9}$, no solution.

Step 2.2: $x = 3k+2$

$(3k+2)^3 - (3k+2)^2 - (3k+2) + 4 \equiv 0 \pmod{9}$

$\Rightarrow \cancel{27}k^3 + \cancel{54}k^2 + \cancel{36}k + 8 - \cancel{9}k^2 - 12k - 4 - 3k - 2 + 4 \equiv 0 \pmod 9$

$\Rightarrow -15k + 6 \equiv 0 \pmod 9$

$\Rightarrow -5k + 2 \equiv 0 \pmod 3$

$\Rightarrow k + 2 \equiv 0 \pmod 3$

$\Rightarrow k \equiv 1 \pmod 3$

$\Rightarrow x = 3k + 2 = 3 \cdot (3\ell + 1) + 2 = 9\ell + 5.$

<u>Step 3</u> : $x = 9\ell + 5$

$(9\ell+5)^3 - (9\ell+5)^2 - (9\ell+5) + 4 \equiv 0 \pmod{27}$

$\Rightarrow \cancel{9^3\ell^3} + \cancel{3 \cdot 9^2 \cdot \ell^2} \cdot 5 + \cancel{3 \cdot 9 \cdot \ell} \cdot 5^2 + 125 - \cancel{81}\ell^2 - 90\ell - 25 - 9\ell - 5 + 4$
$\equiv 0 \pmod{27}$

$\Rightarrow -99\ell + 99 \equiv 0 \pmod{27}$

$\Rightarrow -11\ell + 11 \equiv 0 \pmod 3$

$\Rightarrow \ell + 2 \equiv 0 \pmod 3$

$\Rightarrow \ell \equiv 1 \pmod 3$

$x = 9\ell + 5 = 9 \cdot (3m + 1) + 5 = 27m + 14.$

$x \equiv 14 \pmod{27}.$

<u>Hensel's Lemma:</u> If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $0 \leqslant t \leqslant p-1$ such that $f(a+t\cdot p^j) \equiv 0 \pmod{p^{j+1}}$

- What does it mean? If $a \pmod{p}$ is a solution, then a can be lifted uniquely to mod p^2, and to mod p^3, ..., to mod p^k when $f'(a) \not\equiv 0 \pmod{p}$

- $f(x) = x^3 - x^2 - x + 4$ $\qquad f(2) \equiv 0 \pmod{3}$

  $f'(x) = 3x^2 - 2x - 1$ $\qquad f'(2) \not\equiv 0 \pmod{3}$

$$\Rightarrow 2 \pmod{3} \rightarrow 14 \pmod{27}$$

However, $f'(1) \equiv 0 \pmod{3}$ and we couldn't lift 1 mod 3 to mod 27.

Before proving Hensel's Lemma,

Binomial Theorem:

$$(x+y)^n = \underbrace{x^n}_{\binom{n}{0}=1} + \underbrace{n}_{\binom{n}{1}} \cdot x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \ldots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} \cdot y^n$$

e.g. $(x+y)^5 = x^5 + 5x^4 y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$

Proof of Hensel : $f(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_1 x + c_0$.

We have $f(a) \equiv 0 \pmod{p^j}$

$$f(a + t \cdot p^j) = c_d \cdot (a + t \cdot p^j)^d + c_{d-1} \cdot (a + t \cdot p^j)^{d-1}$$

$$+ \dots + c_2 \cdot (a + t \cdot p^j)^2 + c_1 \cdot (a + t \cdot p^j) + c_0$$

- With Binomial Theorem

$(a + t p^j)^d \equiv a^d + d \cdot a^{d-1} \cdot t p^j +$ something divisible by p^{j+1}

$$\equiv a^d + d \cdot a^{d-1} \cdot t p^j \pmod{p^{j+1}}$$

$$f(a + t p^j) \equiv c_d \cdot (a^d + d a^{d-1} t p^j) + c_{d-1} (a^{d-1} + (d-1) a^{d-2} t p^j)$$

$$+ \dots + c_2 \cdot (a^2 + 2 a t p^j) + c_1 \cdot (a + t p^j) + c_0$$

$$\equiv (c_d a^d + c_{d-1} a^{d-1} + \dots + c_2 a^2 + c_1 a + c_0)$$

$$+ t p^j (c_d \cdot d \cdot a^{d-1} + c_{d-1} (d-1) a^{d-2} + \dots + c_2 \cdot 2 \cdot a + c_1)$$

$$\equiv f(a) + t p^j \cdot f'(a) \pmod{p^{j+1}}$$

$f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$ means

$f(a) + t \cdot p^j \cdot f'(a) \equiv 0 \pmod{p^{j+1}}$

Write $f(a) = p^j \cdot k$

$p^j \cdot k + t \cdot p^j \cdot f'(a) \equiv 0 \pmod{p^{j+1}}$

$k + t \cdot f'(a) \equiv 0 \pmod{p}$.

We proved $f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$
if and only if $k + t \cdot f'(a) \equiv 0 \pmod{p}$

If $f'(a) \not\equiv 0 \pmod{p}$, then there is a
unique solution t. ■

Actually, we proved something more.

<u>Hensel's Lemma (continued)</u> : Let $f(a) \equiv 0 \pmod{p^j}$
and $f'(a) \equiv 0 \pmod{p}$

Case 1 : $\frac{f(a)}{p^j} \not\equiv 0 \pmod{p} \Rightarrow a$ cannot be lifted
to mod p^{j+1}.

Case 2 : $\frac{f(a)}{p^j} \equiv 0 \pmod{p} \Rightarrow f(a + t p^j) \equiv 0 \pmod{p}$
for all $t = 0, 1, \ldots, p-1$, i.e. a can be lifted
to p solutions in mod p^{j+1}.

Remark: When $f'(a) \equiv 0 \pmod{p}$, either every lift is a solution or none of them is a solution.

Counting solutions with Hensel

① $x^3 - x^2 + 4x + 1 \equiv 0 \pmod{125}$

In mod 5, $f(1) \equiv f(4) \equiv 0 \pmod{5}$

$f'(x) = 3x^2 - 2x + 4$.

$f'(1) \equiv 0 \pmod{5}$ $\qquad$ $f'(4) \not\equiv 0 \pmod{5}$

$\downarrow$ $\qquad$ $\downarrow$

no solution $\qquad$ unique solution in $\mathbb{Z}_{125}$

$\frac{f(1)}{5} \not\equiv 0 \pmod{5}$

$\Rightarrow$ One solution in $\mathbb{Z}_{125}$.

We'll continue with more examples on Wednesday.