Lucas' Thm:

If n is an integer and for every prime p with $p \mid n-1$, there is an a with

$$a^{n-1} \underset{n}{\equiv} 1 \quad \text{and} \quad a^{\frac{n-1}{p}} \underset{n}{\not\equiv} 1,$$

then n is prime.

Note $a^{n-1} \underset{n}{\equiv} 1 \Rightarrow (a,n)=1$ So $a^{\phi(n)} \underset{n}{\equiv} 1$.

Pf: Suppose n is not prime. Then $\phi(n) = \#$ of $1 \le a \le n$ with $(a,n)=1$ is $< n-1$. Therefore there is a prime q and an $r \ge 1$ with $q^r \nmid \phi(n)$, $q^r \mid n-1$. Then pick the a for which

$$a^{n-1} \underset{n}{\equiv} 1, \quad a^{\frac{n-1}{q}} \underset{n}{\not\equiv} 1.$$

Let $\overset{m}{\overset{\parallel}{\text{ord}_n(a)}} =$ smallest k s.t. $a^k \underset{n}{\equiv} 1$.

Then ~~...~~ $\qquad n = xq^r$

$\text{ord}_n(a) \mid \phi(n)$ ~~...~~ $\qquad (x,q)=1$

$\longrightarrow q^r \nmid \text{ord}_n(a) \qquad m \mid xq^r, \quad m \nmid xq^{r-1}$

But $\quad m = q^s b \quad (q,b)=1$

If $s < r$ then $\Longrightarrow$ ~~$aq \cdot mx$~~

$\frac{m}{q^s} = b \mid xq^{r-s}$ contrad. ~~$aq^{r-1} = my + b$~~

$(b,q)=1 \Rightarrow b \mid x$ ~~$mx = aq = mq + bq$~~

$\Rightarrow b \mid xq^{r-s-1}$

$\Rightarrow m \mid xq^{r-1}$ ~~$(x-aq) = bq$~~

Fast primality tests for special cases

__Fact:__ If p is prime, then there is an a with $a^{p-1} \underset{p}{\equiv} 1$ but $a^k \underset{p}{\not\equiv} 1$ for any $k < p-1$. [a = "primitive root of unity"]

~~Proof~~: __Need:__

Fact: (Lagrange's Thm) If $f(x) = a_n x^n + \dots + a_0$ is a poly w/ integer coeffs and p is __prime__, then the eqn $f(x) \underset{p}{\equiv} 0$ has __at most__ n solutions (mod p) ($n \geq 1$, $a_n \underset{p}{\not\equiv} 0$)

Pf: Induction on n.

$n=1$ $\quad ax+b \equiv 0 \pmod p$ $\quad ax \underset{p}{\equiv} -b$ $\quad a\bar{a} \underset{p}{\equiv} 1$ $\quad x \underset{p}{\equiv} (-b)\bar{a}$

If $n > 1$ and $f(c) \underset{p}{\equiv} 0$ then

$$f(x) = (x-c)g(x) + r$$

degree of $g(x) \leq n-1$ Thus

$$f(x) \underset{p}{\equiv} 0$$

$f(c) = 0 \cdot g(c) + r \underset{p}{\equiv} 0 \implies r \underset{p}{\equiv} 0$ So

$f(x) \underset{p}{\equiv} 0 \iff (x-c)g(x) \underset{p}{\equiv} 0 \iff$

$x - c \underset{p}{\equiv} 0$ __or__ $g(x) \underset{p}{\equiv} 0$ — at most $n-1$ solutions

$\Downarrow$

$x \underset{p}{\equiv} c$

$\implies$ at most n solutions.

If p is prime and $d \mid p-1$ then

$x^{d}-1 \underset{p}{\equiv} 0$ has <u>exactly</u> d solutions.

Pf $\quad x^{p-1}-1 = (x^{d}-1)\,q(x)$ $\qquad$ degree $q(x) \doteq (p-1)-d$

$\Rightarrow$ has $\le (p-1)-d$ solution

$x^{p-1}-1 = (x^{d})^{e}-1$

has $p-1$ solutions

$\Rightarrow x^{d}-1 \underset{p}{\equiv} 0$ has at <u>least</u> d solns

$\Rightarrow$ exactly d.

~~[illegible]~~

~~[illegible]~~

$\sum_{\substack{r \text{ prime} \\ r \mid d}}$

p prime, then there is an a with $a^{p-1} \underset{p}{\equiv} 1$ but

$a^d \underset{p}{\not\equiv} 1$ for any $d < p-1$. note $a^d \underset{p}{\equiv} 1 \Rightarrow d \mid p-1$

Proof:

$x^d \underset{p}{\equiv} 1$ has exactly d solutions. So if we

write $p-1 = p_1^{n_1} \cdots p_k^{n_k}$ $p_1 < \cdots < p_k$ prime then

$x^{p_i^{n_i}} \underset{p}{\equiv} 1$ has more solutions than $x^{(p_i^{n_i - 1})} \underset{p}{\equiv} 1$.

Pick one, a_i so $a_i^{p_i^{n_i}} \underset{p}{\equiv} 1$ but $a_i^{p_i^{n_i-1}} \underset{p}{\not\equiv} 1$.

Set $a = a_1 \cdots a_k$. Then ie. $\mathrm{ord}_p(a_i) = p_i^{n_i}$

$$a^{p-1} = (a_1 \cdots a_k)^{p_1^{n_1} \cdots p_k^{n_k}} = \left(a_1^{p_1^{n_1}}\right)^{\text{rest}_1} \left(a_2^{p_2^{n_2}}\right)^{\text{rest}_2} \cdots$$
$$= 1 \cdots 1 = 1$$

But

$$a^{\frac{p-1}{p_i}} = 1 \cdots \left(a_i^{(p_i^{n_i-1})}\right)^{\overline{\quad}} \cdots 1 \underset{p}{\not\equiv} 1$$

b/c $p_i^{n_i} \nmid$ ———

So a is a primitive root!

The first prime p of the form $326n^2+3$ for which $\mathrm{ord}_p(326) \neq p-1$ has $p \geq 10^7$

Fact: There are actually $\phi(p-1)$ (incongruent) primitive roots mod p. [We will need to understand $\phi(n)$ a lot better to see why...]

For example (think of numbers n for which $n-1$ is easy to factor!)

$$n = 2^k+1.$$

Note: n prime $\Longrightarrow k = 2^r$ some r

b/c if $k = 2^r d$ d odd, $d \geq 3$ then

$$2^k+1 = (2^{2^r})^d+1 = a^d+1 \qquad d \text{ odd } \geq 3$$

$$= (a+1)(a^{d-1} \ldots \quad \text{but } (a+1) \mid a^d+1$$

(b/c $(-1)^d+1 = 0$ & $(x+1)$ divides x^d+1.)

A prime of the form $p = 2^{(2^r)}+1$ is called a Fermat prime

Fermat claimed these were prime for all $r \geq 1$, but he was wrong:

$$641 \mid 2^{(2^5)}+1$$

[Pf: (Euler)

$$2^{32}+1 = 2^4 \cdot 2^{28}+1 = 16 \cdot 2^{28}+1 = (641-625) \cdot 2^{28}+1$$

$$= 641 \cdot 2^{28} - 5^4 \cdot 2^{28}+1 = 641 \cdot 2^{28} - (\underbrace{5\, 2^7}_{5 \cdot 128})^4+1$$

$$= 641 \cdot 2^{28} - (640)^4+1$$

$$= 641 \cdot 2^{28} - ((640)^4 - 1^4)$$

$$= 641 \cdot 2^{28} - (((640)^2-1)((640)^2+1))$$

$$= 641 \cdot 2^{28} - 641 \cdot 639 \cdot ((640)^2+1)$$

$$= 641 (2^{28} - 639 \cdot ((640)^2+1))$$