A

Euler Thm: If $(a,n)=1$ then $a^{\varphi(n)} \underset{n}{\equiv} 1$.

FLT: If p is prime and $(a,p)=1$ then $a^{p-1} \underset{p}{\equiv} 1$

Contrapositive: If $a^{p-1} \underset{p}{\not\equiv} 1$ then either p isn't prime or $(a,p)\geq 2$

Detects non-primes.

Wilson's Thm

$$p \text{ is prime} \iff (p-1)! \underset{p}{\equiv} -1.$$

Did $\Leftarrow$

Proof:

($\Rightarrow$) Some useful prelim facts:

Lemma: If ~~p is prime and~~ $(a,p)=1$ then $\exists\, x \in \mathbb{N}$ with $ax \underset{p}{\equiv} 1$.

[$x = a^{\varphi(p)-1}$, or $ax+py=1 \Rightarrow ax \underset{p}{\equiv} 1$.]

Lemma: if $(a,p)=1$ and $ax \underset{p}{\equiv} ay$ then $x \underset{p}{\equiv} y$

Lemma: If $x^2 \underset{p}{\equiv} 1$ with p prime, then $x \underset{p}{\equiv} 1$ or $x \underset{p}{\equiv} -1$.

[Pf: $p \mid x^2-1 = (x-1)(x+1) \Longrightarrow p \mid x-1$ or $p \mid x+1$.]

Now, $(p-1)! = 1\cdot 2\cdot 3 \cdots (p-2)(p-1)$.

For each $a = 2,\dots,p-2$ there is exactly one $a' \in \{2,\dots,p-2\}$ with $aa' \underset{p}{\equiv} 1$. (Note: $a \underset{p}{\not\equiv} a'$, since then $a^2 \underset{p}{\equiv} 1$.) Then we can pair up the #s $2,\dots,p-2$

$\{2,\dots,p-2\} = \{a_1,a_1'\} \cup \cdots \cup \{a_k,a_k'\}$ with $a_i a_i' \underset{p}{\equiv} 1$.

then $2\cdots(p-2) \underset{p}{\equiv} (a_1a_1')\cdots(a_ka_k') \underset{p}{\equiv} 1^k = 1$.

So $(p-2)! \underset{p}{\equiv} 1$, so $(p-1)! = (p-2)!(p-1) \underset{p}{\equiv} 1\cdot(p-1) = p-1 \underset{p}{\equiv} -1$

OTOH, if p isn't prime, then $p=ab$ $a,b \geq 2$. (WLOG $a \leq b$)
If $p=4=2\cdot 2$ then $(p-1)! = 6 \underset{4}{\equiv} 2 \not\equiv -1$.
If $p>4$ then if $a \neq b$, then $a,b \leq p-1$ so $ab \mid (p-1)!$ so $(p-1)! \underset{p}{\equiv} 0$. If $a=b\geq 3$ then $a, 2a \leq p-1$ so $a\cdot 2a = 2a^2 \mid (p-1)! \implies (p-1)! \underset{p}{\equiv} 0$.

If p is prime and $p \underset{4}{\equiv} 1$, then the eqn $x^2 \underset{p}{\equiv} -1$ has a solution.

By Wilson's Thm, $(p-1)! \underset{p}{\equiv} -1$. But $p-1 \underset{4}{\equiv} 0$ so $2 \mid \frac{p-1}{2}$

$$-1 \underset{p}{\equiv} (p-1)! = \left(1\cdot 2 \cdots \tfrac{p-1}{2}\right)\left(\tfrac{p+1}{2} \cdots (p-2)(p-1)\right)$$
$$= \left(\prod_{k=1}^{\frac{p-1}{2}} k\right)\left(\prod_{k=1}^{\frac{p-1}{2}} (p-k)\right) = \prod_{k=1}^{\frac{p-1}{2}} (k)(p-k) \underset{p}{\equiv} \prod_{k=1}^{\frac{p-1}{2}} (-1)(k^2)$$
$$= (-1)^{\frac{p-1}{2}}\left(\prod_{k=1}^{\frac{p-1}{2}} k\right)^2 = \left(\prod_{k=1}^{\frac{p-1}{2}} k\right)^2 = x^2.$$

OTOH, if p is prime and $x^2 \underset{p}{\equiv} -1$ then ($p=2$ and $-1 \underset{2}{\equiv} 1$ so $x=1$ works or) p is odd, $\frac{p-1}{2} = n$ is an integer, ~~thus~~ and

$$(x^2)^{\frac{p-1}{2}} = x^{p-1} \underset{p}{\equiv} 1. \text{ So } (-1)^{\frac{p-1}{2}} \underset{p}{\equiv} 1 \text{ so}$$
$$\underset{p}{\equiv}$$
$$(-1)^{\frac{p-1}{2}}$$

$(-1)^{\frac{p-1}{2}} = 1$ so $\frac{p-1}{2}$ is even,
$\frac{p-1}{2} = 2r$; $p = 4r+1$; $p \underset{4}{\equiv} 1$

So $x^2 \underset{p}{\equiv} -1$ has a soln (p prime) $\iff p=2$ or $p \underset{4}{\equiv} 1$.

If p is prime and $p \underset{4}{\equiv} 1$, then $p = a^2+b^2$ for some $a,b \in \mathbb{Z}$.

By the above, there is an $x \in \mathbb{Z}$ with $x^2 \underset{p}{\equiv} -1$.

Set $k = \lfloor \sqrt{p} \rfloor = \max\{n \in \mathbb{Z} : n \le \sqrt{p}\}$ $k \ne \sqrt{p}$ (o/w $p = k^2$ is not prime!) so $k < \sqrt{p} < k+1$.

Look at

$$u + xv \quad \text{with} \quad 0 \le u, v \le k$$

There are a total of $(k+1)^2 > p$ integers. So two of them must be $\underset{p}{\equiv}$; $u + xv \underset{p}{\equiv} u' + xv'$

then $a = u - u' \underset{p}{\equiv} x(v' - v) = xb$, so

$$a^2 \underset{p}{\equiv} x^2 b^2 \underset{p}{\equiv} (-1) b^2. \quad \text{So} \quad p \mid a^2 + b^2.$$

But $u, u' \in \{0, \dots, k\} \Rightarrow |u - u'| \le k$ Similarly $|v - v'| \le k$

so $0 < a^2 + b^2 \le k^2 + k^2 = 2k^2 < 2p$. So $0 < a^2 + b^2 < 2p$ and $p \mid a^2+b^2$.

So $p = a^2 + b^2$!

[illegible]

OTOH: If $p \equiv_4 3$ and is prime and $p \mid a^2+b^2$, then $p \mid a$ and $p \mid b$. (*)

If not, WOLOG $p \nmid a$ so $(p,a)=1$. So $\exists\, x$ with $ax \equiv_p 1$. Then

$$x^2(a^2+b^2) \equiv_p x^2 \cdot 0 = 0$$
$$\parallel$$
$$(ax)^2+(bx)^2 \equiv_p 1^2+(bx)^2$$

So $(bx)^2 \equiv_p -1$, which is impossible!

Since $2 = 1^2+1^2$ is a sum of 2 squares, and

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 \quad \underline{\text{and}}$$

$$p^2 = p^2+0^2$$

<u>Any</u> n whose prime factorization $n = p_1^{k_1} \cdots p_r^{k_r}$ $p_1 < \cdots < p_r$ has k_i even for each $p_i \equiv_4 3$ can be expressed as $n = a^2+b^2$, <u>and</u> <u>conversely</u>.

B/c $n = a^2+b^2$ and $p \mid n$, $p \equiv_4 3$, p prime $\Rightarrow$ ~~$p^2 \mid a$~~ $p \mid a$, $p \mid b$

so $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$ and <u>repeat</u>!