As $t f'(3) \equiv \frac{-f(3)}{7} \pmod 7$ becomes

$$t \equiv -5 \pmod 7$$
$$t \equiv 2 \pmod 7$$

Thus, we obtain one solution (as we should since $p \nmid f'(3)$) given by

$$y = 3 + 2(7) = 17 \pmod{49}.$$

□

We will come back to solving polynomial congruences when we study quadratic reciprocity. Our next step in developing the necessary background is studying Fermat's Little Theorem.

Thm 5.1: (Fermat's Little Theorem) Let p be a prime number. Then $a^p \equiv a \pmod p$ for any $a \in \mathbb{Z}$.

We will give a couple of proofs of this fact. The first we will give is using abstract algebra.

Proof 1: Recall that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group with $p-1$ elements. Thus, $a^{p-1} \equiv 1 \pmod p$ for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. This gives the result for any $a \in \mathbb{Z}$ with $\gcd(a,p) = 2$ upon multiplying by a. If $\gcd(a,p) > 1$, then

$a \equiv 0 \pmod p$ and clearly $a^p \equiv 0^p \equiv 0 \pmod p$. Thus, the result is true for all $a \in \mathbb{Z}$. ∎

Our second proof uses induction and relies on the following lemma.

Lemma: Let p be prime and $1 \le k \le p-1$. Then $p \mid \binom{p}{k}$.

Proof: Recall that

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k!}.$$

Thus,

$$k! \binom{p}{k} = p(p-1)\cdots(p-k+1).$$

It is clear that $p \mid (p(p-1)\cdots(p-k+1))$, so $k!\binom{p}{k} \equiv 0 \pmod p$. Since p is prime, $p \mid k!$ or $p \mid \binom{p}{k}$.

$p \nmid k!$ since $k \le p-1$, thus $p \mid \binom{p}{k}$ as desired. ∎

Proof 2 of F. Little Thm: We proceed by induction on a. The case $a = 0$ or $a = 1$ are both trivial. Now suppose the result holds for all $1 \le k \le a$ with $a \in \mathbb{Z}_{\ge 0}$.

We have

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1$$

$$\equiv a^p + 1 \pmod p \qquad \text{(by lemma)}$$

$$\equiv a + 1 \pmod p \qquad \text{(by ind. hyp)}$$

Thus, $a^p \equiv a \pmod p$ $\forall\ a \geq 0$ by strong induction. To get the result for $a < 0$, we use that $a \equiv r \pmod p$ for some $0 \leq r \leq p-1$, so

$$a^p \equiv r^p \equiv r \equiv a \pmod p.$$

Thus, the result holds for all $a \in \mathbb{Z}$. ∎

Proof 3: Consider the integers $a, 2a, \ldots, (p-1)a$. Our first claim is none of these are congruent to one another mod p if $\gcd(p,a) = 1$. If so, say $i\,a \equiv j\,a \pmod p$, then since $\gcd(a,p) = 1$ we can cancel the a to obtain $i \equiv j \pmod p$. Thus, $i = j$ since i and j are both less than p and greater than 0.

The pigeonhole principle gives that

$$\{a, 2a, \ldots, (p-1)a\} = \{1, 2, \ldots, p-1\}$$

for $\gcd(a,p) = 1$. Thus,

$$a \cdot 2a \cdot 3a \cdots (p-1)a = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p,$$

i.e., $a^{p-1}(p-1)! \equiv (p-1)! \pmod p$. Since $\gcd(p, (p-1)!) = 1$, we can cancel the $(p-1)!$ to obtain

$$a^{p-1} \equiv 1 \pmod p$$

if $\gcd(a,p) = 1$. Multiply through by a to get the desired form.

If $\gcd(a,p) > 1$, then $a \equiv 0 \pmod{p}$ and clearly the result is true. ∎

Before we study some applications of Fermat's little theorem, we give a natural generalization. We begin by defining Euler's φ function, which will we study further in the future.

Def: Let n be a positive integer. Euler's φ-function is defined by $\varphi(n) = \#$ of positive integers less than n that are relatively prime to n.

Example: $\varphi(5) = 4$

$\varphi(8) = 4$

$\varphi(77) = 60$

The command is

```
euler_phi(n)
```

in SAGE.

Thm: Let m and n be relatively prime positive integers. Then $\varphi(mn) = \varphi(m)\varphi(n)$. If

$$m = p_1^{e_1} \cdots p_r^{e_r}$$

then

$$\varphi(m) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = m \prod_{i=1}^{r} (1 - 1/p_i).$$

This theorem is showing that φ is what is known as an a multiplicative function.

Proof: Let $n = n_1 n_2$. Suppose x is such that $\gcd(x, n) = 1$.

Reducing x modulo n_1 gives an a_1 with $0 < a_1 < n_1$, $\gcd(a_1, n_1) = 1$, and $x \equiv a_1 \pmod{n_1}$. Similarly, we get a_2 with $0 < a_2 < n_2$, $\gcd(a_2, n_2) = 1$, and $x \equiv a_2 \pmod{n_2}$. Note that $\gcd(a_i, n_i) = 1$ b/c $\gcd(x, n_i) = 1$ and $x \equiv a_i \pmod{n_i}$. Thus we see that for any x we obtain a pair (a_1, a_2) s.t $\gcd(a_i, n_i) = 1$ and $1 \le a_i \le n_i$. Thus, we must have $\varphi(n) \le \varphi(n_1)\varphi(n_2)$.

Now let (a_1, a_2) be a pair of integers so that $1 \le a_i < n_i$, $\gcd(a_i, n_i) = 1$. The chinese remainder theorem gives an x s.t

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

with $1 \le x < n_1 n_2$. Since $\gcd(n_i, a_i) = 1$, we have $\gcd(x, n_i) = 1$. Thus, we see that for each pair (a_1, a_2) w/ $1 \le a_i < n_i$, $\gcd(a_i, n_i) = 1$, we obtain a unique x s.t. $\gcd(x, n_i) = 1$ and $1 \le x < n_1 n_2$.

(Note $\gcd(x, n) = 1$ necessarily!) Thus, $\varphi(n_1)\varphi(n_2) \le \varphi(n)$ and so we have shown $\varphi(n) = \varphi(n_1)\varphi(n_2)$.

Now let $n = p_1^{e_1} \cdots p_r^{e_r}$. Repeatedly applying what we have just shown gives

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{e_i}).$$

Thus, we only need to compute $\varphi(p^e)$ for p a prime and $e \geq 1$. Let a be an integer with $1 \leq a \leq p^e$. Then $\gcd(a, p^e) = 1$ unless a happens to be

$$p,\ 2p,\ 3p,\ \ldots,\ p^{e-1} \cdot p .$$

There are precisely p^{e-1} such numbers. Thus, there are $p^e - p^{e-1}$ integers a with a relatively prime to p^e and $1 \leq a \leq p^e$. Thus,

$$\varphi(p^e) = p^e - p^{e-1}$$

$$= p^e\left(1 - \frac{1}{p}\right).$$

This gives the desired result. ∎

<u>Thm: (Euler's Thm):</u> Let n be a positive integer and $a \in \mathbb{Z}$ s.t. $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

<u>Proof:</u> As with Fermat's little theorem, this follows easily if we use abstract algebra noting that the group $(\mathbb{Z}/n\mathbb{Z})^\times$ has order $\varphi(n)$. ∎

To prove Euler's Theorem without abstract algebra we need a little set-up.

Def: Let $m > 1$ be an integer. A *reduced residue system modulo m* is a set of integers x_i s.t. $\gcd(x_i, m) = 1$, $x_i \not\equiv x_j \pmod{m}$ if $i \neq j$, and every integer x that is relatively prime to m is congruent to x_i for some i.

Lemma: Let $a \in \mathbb{Z}$ s.t. $\gcd(a, m) = 1$. Let $x_1, \ldots, x_{\varphi(m)}$ be a reduced residue system modulo m. Then $ax_1, \ldots, ax_{\varphi(m)}$ is a reduced residue system modulo m.

Proof: This is an easy exercise!

Proof (Euler's Thm): Let $x_1, \ldots, x_{\varphi(m)}$ be a reduced residue system modulo m. Then $ax_1, \ldots, ax_{\varphi(m)}$ is also a reduced residue system modulo m. Thus, for each i there is exactly one j s.t.

$$x_i \equiv a x_j \pmod{m},$$

Thus,

$$\{x_1, \ldots, x_{\varphi(m)}\} = \{ax_1, \ldots, ax_{\varphi(m)}\}.$$

So we have

$$a x_1 \cdots a x_{\varphi(m)} \equiv x_1 \cdots x_{\varphi(m)} \pmod{m}$$

i.e.,

$$a^{\varphi(m)} x_1 \cdots x_{\varphi(m)} \equiv x_1 \cdots x_{\varphi(m)} \pmod{m}.$$

Since $\gcd(x_i, m) = 1$ for each i, we can cancel $x_1 \cdots x_{\varphi(m)}$ to obtain the result. ∎

Our first application of Fermat's little theorem is to studying quadratic congruences. We are able to obtain some preliminary results before studying quadratic reciprocity. We will then use Fermat's little theorem to study public-key cryptography.

<u>Lemma:</u> Let p be a prime number. Then $x^2 \equiv 1 \pmod{p}$ iff $x \equiv \pm 1 \pmod{p}$.

<u>Proof:</u> If $x \equiv \pm 1 \pmod{p}$, then clearly $x^2 \equiv 1 \pmod{p}$.

If $x^2 \equiv 1 \pmod{p}$, then $x^2 - 1 \equiv 0 \pmod{p}$. Thus, $p \mid (x^2 - 1) = (x-1)(x+1)$. Using that p is prime gives $p \mid (x-1)$ or $p \mid (x+1)$, i.e., $x \equiv \pm 1 \pmod{p}$. ∎

We now need Wilson's theorem for our next result.

Thm 5.4: Let p be a prime. Then $(p-1)! \equiv -1 \pmod{p}$.

Proof: The result is clear for $p = 2, 3$, so we may assume $p \geq 5$. Let $a \in \mathbb{Z}$ s.t. $1 \leq a \leq p-1$. Since $\gcd(a,p) = 1$, there is a unique $\bar{a} \in \mathbb{Z}$ s.t. $1 \leq \bar{a} \leq p-1$ and

$$a\bar{a} \equiv 1 \pmod{p}.$$

(linear congruence results). Thus, a and $\bar{a}$ form a pair s.t. $\bar{a}\bar{a} \equiv 1 \pmod{p}$. Thus, their contribution to $(p-1)!$ is 1. The only thing we need to worry about is if $a = \bar{a}$. But this happens only if $a^2 \equiv 1 \pmod{p}$, i.e., from our previous result if $a \equiv 1, p-1 \pmod{p}$. Thus, if we pull off the 1 and $p-1$ from $(p-1)!$, we can pair off the rest of the terms as above

$$\begin{aligned}(p-1)! &\equiv (p-1) \cdot \prod a\bar{a} \cdot 1 \pmod{p} \\ &\equiv p-1 \pmod{p} \\ &\equiv -1 \pmod{p}.\end{aligned}$$

□

We can apply Wilson's theorem (Thm 5.4) to deduce the following theorem, a special case of quadratic reciprocity.

Thm 5.5: Let p be a prime. The congruence

$$x^2 \equiv -1 \pmod{p}$$

has solutions iff $p=2$ or $p \equiv 1 \pmod{4}$.

Proof: If $p=2$, then $-1 \equiv 1$ and so $x=1$ provides a solution. We may now assume p is an odd prime.

We rewrite Wilson's theorem as

$$(1 \cdot 2 \cdots \tfrac{p-1}{2})(\tfrac{p+1}{2} \cdots (p-1)) \equiv -1 \pmod{p}. \quad (*)$$

Rewriting again we have

$$\prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1 \pmod{p}.$$

Here we have just paired off the terms in $(*)$.

Observing that $j(p-j) \equiv -j^2 \pmod{p}$, we have

$$\prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} -j^2 \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j^2 \pmod{p}.$$

Now if $p \equiv 1 \pmod{4}$, $\exists\, m \in \mathbb{Z}$ s.t. $p-1 = 4m$.

Thus, $(-1)^{\frac{p-1}{2}} = (-1)^{2m} = 1$. So if we set $x = (\tfrac{p-1}{2})!$, then this provides a solution to the congruence since we will have

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 = \prod_{j=1}^{\frac{p-1}{2}} (j^2)$$

$$\equiv \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \pmod{p}$$

$$\equiv -1 \pmod{p}.$$

Suppose conversely now that x is a solution of $x^2 \equiv -1 \pmod{p}$.

Clearly $p \nmid x$. If $p = 2$ we are done, so suppose $p > 2$.

Then raising both sides of the congruence to $\left(\frac{p-1}{2}\right)$ we have

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

However, Fermat's little theorem gives $x^{p-1} \equiv 1 \pmod{p}$.

So we must have

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Now $(-1)^{\frac{p-1}{2}} = \pm 1$ and $-1 \not\equiv 1 \pmod{p}$ $(p > 2)$

and so we must have that $(-1)^{\frac{p-1}{2}} = 1$, not just congruent. But this is equivalent to $\frac{p-1}{2}$ is even, i.e. $p - 1 = 4m$ for some m. ∎

Note that this theorem and the following ones are normally encountered in an abstract algebra class when studying $\mathbb{Z}[i]$, the Gaussian integers.

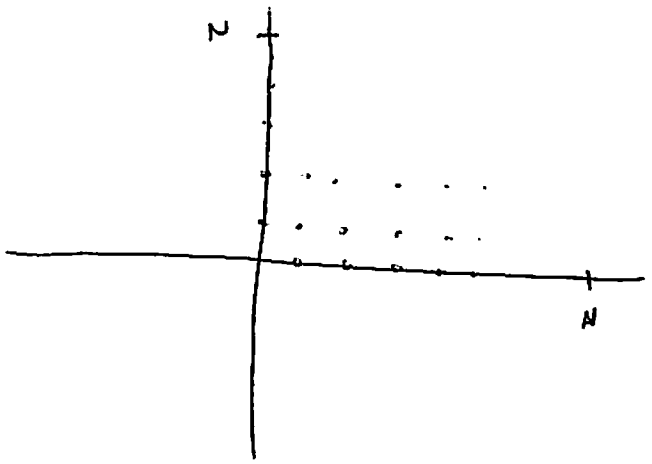
Cor: Let p be a prime number with $p \equiv 1 \pmod 4$.

Then $\exists\ a, b \in \mathbb{Z}_{>0}$ s.t. $p = a^2 + b^2$.

Proof: We apply the previous theorem to conclude $\exists\ x \in \mathbb{Z}$ s.t. $x^2 \equiv -1 \pmod p$. Define a function

$$f(u,v) = u + xv.$$

Let $N = \lfloor \sqrt{p} \rfloor$. (Recall $\lfloor y \rfloor$ is the greatest integer less than or equal to y, i.e., $\lfloor y \rfloor \le y < \lfloor y \rfloor + 1$.) Since p is prime, $\sqrt{p} \notin \mathbb{Z}$ and so $N < \sqrt{p} < N+1$. We consider the set of integer pairs (u,v) with $0 \le u \le N$, $0 \le v \le N$.



The values u and v each take $N+1$ values, so we have $(N+1)^2$ different pairs (u,v). Since $N+1 > \sqrt{p}$, we have more than p pairs. The pigeonhole principle then gives that we must have $f(u,v)$ is congruent modulo p to $f(m,n)$ for some u, v, m, n in our range, $(u,v) \neq (m,n)$.

Thus, we have

$$f(u,v) \equiv f(m,n) \pmod p.$$

i.e.,

$$u+xv \equiv m+xn \pmod{p}.$$

Hence,

$$u-m \equiv x(n-v) \pmod{p}.$$

Set $a = u-m$, $b = v-n$. Then

$$a \equiv -bx \pmod{p}.$$

Square both sides:

$$\begin{aligned} a^2 &\equiv (-bx)^2 \pmod{p} \\ &\equiv b^2x^2 \pmod{p} \\ &\equiv -b^2 \pmod{p}. \end{aligned}$$

Thus, $a^2+b^2 \equiv 0 \pmod{p}$. Hence we have $p \mid (a^2+b^2)$.

Since $(u,v) \neq (m,n)$, we have $a^2+b^2 > 0$. Now we must show a^2+b^2 cannot be larger than p. Observe that $u \leq N$ and $m \geq 0$, so

$$a = u-m \leq N.$$

Similarly $a \geq -N$. and $-N \leq b \leq N$.

Thus, $|a| \leq \sqrt{p}$ and $|b| \leq \sqrt{p} \Rightarrow$

$$a^2+b^2 < 2p.$$

However, p is the only multiple of p in the range $(0, 2p)$, so it must be that $a^2+b^2 = p$.

□

We would now like to establish the result in the opposite direction; namely, if $\exists\ a,b \in \mathbb{Z}_{>0}$ s.t. $a^2+b^2 = p$, then $p \equiv 1 \pmod 4$ (p an odd prime here of course). We accomplish this with the following lemma.

<u>Lemma:</u> Let q be an odd prime s.t. $q \mid (a^2+b^2)$ for $a,b \in \mathbb{Z}_{>0}$. If $q \equiv 3 \pmod 4$, then $q \mid a$ and $q \mid b$.

Before we prove the lemma, let's see how it gives the converse we are interested in.

Suppose p is an odd prime and $\exists\ a,b \in \mathbb{Z}_{>0}$ s.t. $p = a^2+b^2$. If $p \equiv 1 \pmod 4$ we are done. Since the only other case is $p \equiv 3 \pmod 4$ (p an odd prime) the lemma shows that we would have $p \mid a$ and $p \mid b \Rightarrow p^2 \mid p$. #. Thus, $p \equiv 1 \pmod 4$. So it only remains to prove the lemma.

<u>Proof:</u> Suppose q is an odd prime s.t. $q \mid (a^2+b^2)$ for some $a,b \in \mathbb{Z}_{>0}$ with $q \nmid a$ or $q \nmid b$. WLOG we may assume $q \nmid a \Rightarrow \gcd(a,q) = 1$. Thus $\exists\ m,n \in \mathbb{Z}$ s.t. $am + qn = 1$. Thus, $am \equiv 1 \pmod q$. Since $q \mid (a^2+b^2)$, we have $a^2+b^2 \equiv 0 \pmod q$, i.e.,

$a^2 \equiv -b^2 \pmod{q}$. Multiply both sides by m^2 to obtain

$(am)^2 \equiv -(bm)^2 \pmod{q}$, i.e.

$-(bm)^2 \equiv 1 \pmod{q}$

$\Leftrightarrow (bm)^2 \equiv -1 \pmod{q}$. But then says we have a solution to the congruence

$$X^2 \equiv -1 \pmod{q}$$

$\Rightarrow q \equiv 1 \pmod{4}$. ∎