that is not of the form $4k+3$ that divide N. Odd primes are of the form $4k+1$ or $4k+3$. Since N cannot be divisible by any prime of the form $4k+3$, it must be divisible by prime of the form $4k+1$. However, this contradicts that N is of the form $4m+3$ since $(4k+1)(4l+1) = 4x+1$. ☒

Thus far, everything we have discussed has had to do with divisibility in one form or another. We have basically worked from the definition to gain insights. We will now ~~introduce~~ introduce a new tool, the theory of congruence. This was first established by Gauss. You should read the section in the text for some relevant historical background.

Def: Let $n \in \mathbb{Z}_{>0}$. We say integers a and b are congruent modulo n, written

$$a \equiv b \pmod{n}$$

if $n \mid (a-b)$.

Examples: ① $2 \equiv 9 \pmod{7}$

$6 \equiv -1 \pmod{7}$

② $-5 \equiv 1{,}000{,}250{,}005 \pmod 5$.

③ $m \equiv n \pmod 1 \quad \forall m, n \in \mathbb{Z}$

Thm 4.1: Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod n$ iff a and b leave the same remainder when divided by n.

Proof: "$\Rightarrow$" Let $a \equiv b \pmod n$ and write

$$a = nq_1 + r_1 \qquad 0 \le r_1 < n$$
$$b = nq_2 + r_2. \qquad 0 \le r_2 < n.$$

We have $a - b = n(q_1 - q_2) + (r_1 - r_2)$.

Since ~~as~~ $n \mid (a-b)$ and $n \mid (n(q_1 - q_2))$, we must have $n \mid (r_1 - r_2)$. But $0 \le r_1, r_2 < n$

$\Rightarrow \quad r_1 = r_2$.

"$\Leftarrow$" Suppose a and b leave the same remainder when divided by n. Then we can write

$$a = nq_1 + r$$
$$b = nq_2 + r$$

for some $q_1, q_2, r \in \mathbb{Z}$. Then

$$a - b = n(q_1 - q_2)$$

$\Rightarrow n \mid (a-b) \Rightarrow a \equiv b \pmod n$. ∎

This way of thinking can be useful in solving problems!

~~Consider the following~~

We will see an application in a moment.

We can use Theorem 4.1 combined with the division alg. to conclude that given any integer m, m must be congruent modulo n to $0, 1, 2, .., n-1$, as these are the possible remainders. The set $\{0, 1, .., n-1\}$ is called the set of <u>least nonnegative residues modulo n</u>.

Of course, we can form other sets as well that have the property that every integer must be congruent modulo n to something in the set. For example, $\{n, n+1, .., 2n-1\}$ is another such set since $n \equiv 0 \pmod{n}$, $n+1 \equiv 1 \pmod{n}$, $\ldots, 2n-1 \equiv n-1 \pmod{n}$. Any set $a_1, .., a_n$ of integers with the property that any integer is congruent to one of the a_i's is called a <u>complete residue system modulo n</u>.

We have one more theorem before we see some applications:

<u>Thm 4.2:</u> Let $n > 1$ be fixed and let a, b, c, d be arbitrary integers. Then

① $a \equiv a \pmod{n}$

② If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

③ If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

④ If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

⑤ If $a \equiv b \pmod{n}$, then $a+c \equiv b+c \pmod{n}$ and $ac \equiv bc \pmod{n}$.

⑥ If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ $\forall\ k \geq 0$.

Proof: Let the class pick a couple to see.

Caution: If $ac \equiv bc \pmod{n}$, it is NOT necessarily true that $a \equiv b \pmod{n}$! For example, $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$ but $4 \not\equiv 1 \pmod{6}$! We will come back to this in a moment.

Example: Show that the equation $x^2+y^2=3z^2$ has no nontrivial solutions in the integers.

Proof: Suppose (x,y,z) is such a solution. We can assume $\gcd(x,y,z)=1$ for otherwise we can divide it out. Consider the equation mod 3. We have

$$x^2+y^2 \equiv 0 \pmod{3}.$$

Observe that

$$0^2 \equiv 0 \pmod{3}$$
$$1^2 \equiv 1 \pmod{3}$$
$$2^2 \equiv 1 \pmod{3}$$

We have that 0, 1, 2 form a complete residue system modulo 3, so x and y must each be congruent to one of them. But then to satisfy $x^2+y^2 \equiv 0 \pmod{3}$, we must have $x \equiv 0 \pmod{3}$ and $y \equiv 0 \pmod{3}$. Thus, $3 \mid x$ and $3 \mid y$. So we can write $x = 3k$, $y = 3l$ and the equation becomes

$$3^2(k^2+l^2) = 3z^2$$

$\Rightarrow 3 \mid z$ #. ☒

Example: Find the remainder of $3^{57}-1$ when divided by 8.

Solution: Observe $3^2 \equiv 1 \pmod{8}$. So

$3^{56} = (3^2)^{28} \equiv 1^{28} \equiv 1 \pmod{8}$. Thus

$3^{57}-1 \equiv 3\cdot 1 - 1 \equiv 2 \pmod{8}$. So the remainder is 2.

We now revisit the problem of cancelling across a congruence.

Thm 4.3: If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$ where $d = \gcd(c, n)$.

Proof: Let $ac \equiv bc \pmod{n}$. Then

$$n \mid (ac - bc),$$

so $\exists$ k s.t.

$$nk = ac - bc$$
$$= c(a-b)$$

We know $\exists$ r, s, $\gcd(r,s)=1$, so that $n = dr$, $c = ds$.

$$\Rightarrow \quad drk = ds(a-b)$$

$$\Rightarrow \quad rk = s(a-b)$$

$$\Rightarrow \quad r \mid (a-b).$$

Thus, $a \equiv b \pmod{r} \Rightarrow a \equiv b \pmod{n/d}$. $\blacksquare$

Note that this says if $\gcd(c,n)=1$, then we are free to cancel the c away without worry!

Example: Prove that $27 \mid 2^{5n+1} + 5^{n+2}$ for all $n \geq 1$.

Proof: This is the type of statement we have been proving by induction without using congruences. Let's see how easy it is with congruences. Observe that $2^5 = 32$ and $32 \equiv 5 \pmod{27}$. Thus $2^{5n+1} \equiv 2 \cdot 5^n \pmod{27}$.

$$5^{n+2} = 5^2 \cdot 5^n = 25 \cdot 5^n \equiv -2 \cdot 5^n \pmod{27}.$$

Thus,

$$2^{5n+1} + 5^{n+2} \equiv 2 \cdot 5^n + (-2) \cdot 5^n \pmod{27}$$
$$\equiv 0 \pmod{27}. \quad \blacksquare$$

For another example of how powerful the theory of congruences can be, consider problem 1 from homework 1.

<u>Example:</u> Show $3 \mid 4^n - 1$ for all $n \geq 1$.

<u>Proof:</u> $4^n \equiv 1^n \equiv 1 \pmod{3}$ $\forall n \geq 1$, so $4^n - 1 \equiv 0 \pmod{3}$ $\forall n \geq 1$. ∎

The theory of congruences can also be used to give simple proofs of standard divisibility theorems from grade school.

Recall when we write an integer base 10 such as 5,234 we really mean

$$5 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4.$$

<u>Thm 4.5:</u> Let N be a positive integer with

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 \cdot 10 + a_0.$$

We have $9 \mid N$ iff $9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$.

<u>Proof:</u> We use the fact that $10 \equiv 1 \pmod{9}$ to see

$$N \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}.$$

Now $9 \mid N$ iff $9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$ is clear. ∎

Thm 4.6: Let N be a positive integer with

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 \cdot 10 + a_0.$$

Then $11 \mid N$ iff $11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^n a_n)$.

Proof: We use that $10 \equiv -1 \pmod{11}$. Thus,

$$N \equiv a_n(-1)^n + \cdots + a_1(-1) + a_0 \pmod{11}.$$

We get the result as in the last theorem. $\blacksquare$

Such calculations can be used in real world applications.

Example: International Standard Book Numbers (ISBNs).

These numbers consist of 9 digits $a_1 a_2 \cdots a_9$ and then a 10^{th} digit that is a "check digit" to make sure the others are actually correct and work. The 10^{th} is defined by

$$a_{10} \equiv \sum_{k=1}^{9} k a_k \pmod{11}.$$

The ISBN of our book is 0073051888. We need

$$1\cdot 0 + 2\cdot 0 + 3\cdot 7 + 4\cdot 3 + 5\cdot 0 + 6\cdot 5 + 7\cdot 1 + 8\cdot 8 + 9\cdot 8$$
$$\equiv 8 \pmod{11}.$$

This is true, as can easily be checked.

Suppose we had the problem that two of the numbers in an ISBN were transposed.

Suppose $i<j$ and our ISBN $a_1 \cdots a_i \cdots a_j \cdots a_9 a_{10}$ was accidentally written as $a_1 \cdots a_j \cdots a_i \cdots a_9 a_{10}$. Can we tell this is wrong?

We know that

$$a_1 + 2a_2 + \cdots + ia_i + \cdots + ja_j + \cdots + 9a_9 \equiv a_{10} \pmod{11}.$$

Can

$$a_1 + 2a_2 + \cdots + ia_j + \cdots + ja_i + \cdots + 9a_9 \equiv a_{10} \pmod{11}?$$

Observe that

$$\begin{aligned} a_1 + 2a_2 + \cdots + ia_j + \cdots + ja_i + \cdots + 9a_9 &= a_1 + 2a_2 + \cdots + ia_i + \cdots + ja_j + \cdots + 9a_9 \\ &\quad + (j-i)a_i + (i-j)a_j. \\ &\equiv a_{10} + (j-i)a_i + (i-j)a_j \pmod{11}. \end{aligned}$$

So the question is whether

$$(j-i)a_i + (i-j)a_j \equiv 0 \pmod{11}.$$

Suppose this is the case. Observe that $i-j$ is relatively prime to 11, This is because $1 \le i,j \le 9$ and if $11 \mid (i-j)$, then $i \equiv j \pmod{11}$. $\Rightarrow$ $i=j$. #.

So if $(j-i)a_i + (i-j)a_j \equiv 0 \pmod{11}$, then

$$(j-i)a_i \equiv (j-i)a_j \pmod{11}$$

$$\Rightarrow \quad a_i \equiv a_j \pmod{11} \quad \#.$$

Thus we are able to tell the difference!

As was the case when studying divisibility earlier, now that we have some machinery built up we would like to use it to study solutions to equations. In particular, we would like to look at solutions of equations

$$ax \equiv b \pmod{n}$$

(linear congruences) as well as multiple linear congruences,

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \qquad \vdots \\ x &\equiv a_r \pmod{n_r}. \end{aligned}$$

We begin with linear congruences. We are really only interested in solutions mod n, so if x_0 is a solution then $x_0 + mn$ is a solution for any integer m

$$\left(\begin{aligned} a(x_0 + mn) &= ax_0 + amn \\ &\equiv ax_0 \pmod{n} \\ &\equiv b \pmod{n} \end{aligned} \right)$$

and so is not really any new information. So when we look for solutions, we only look mod n. This shows that

Worst case scenario we could just plug in $x = 0, 1, \ , n-1$ to see if there are any solutions. Of course if n is very large this is not real practical.

Note that x is a solution iff $n \mid ax - b$

iff $\exists$ ~~unique~~ y ~~st~~ $\in \mathbb{Z}$ s.t. $ny = ax - b$

iff ~~ax~~ ~~axxxxxxxx~~ $= ax + n(-y) = b$.

So finding a solution to $ax \equiv b \pmod{n}$ is the same as solving the Diophantine equation $ax + ny = b$.

Thm 4.7: The linear congruence $ax \equiv b \pmod{n}$ has a solution iff $\gcd(a, n) \mid b$. If $\gcd(a, n) \mid b$, then there are $\gcd(a, n)$ noncongruent solutions mod n.

Proof: Let $d = \gcd(a, n)$. Then the first statement is equivalent to our previous result on linear Diophantine equations, this is just phrased in our new language. Now suppose we have a solution x_0. ~~Thengives~~ Remember other solutions then had $x = x_0 + \frac{n}{d} t$ for $t \in \mathbb{Z}$. ~~After those~~ We now need to see for which t these are distinct modulo b. We claim that

$$x_0,\quad x_0+\frac{n}{d},\quad x_0+\frac{2n}{d},\ \dots,\quad x_0+\frac{(d-1)n}{t}$$

are all distinct modulo n. Furthermore, any other

$x_0+\frac{n}{d}t$ must be congruent to one of these.

If we can show this, we will be done.

Suppose $x_0+\frac{n}{d}t_1 \equiv x_0+\frac{n}{d}t_2 \pmod{n}$ w/

$0 \le t_1 < t_2 \le d-1$. Then we have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}.$$

Since $\gcd(\frac{n}{d}, n) = \frac{n}{d}$, we can cancel the $\frac{n}{d}$ to obtain

$$t_1 \equiv t_2 \pmod{d} \cdot \#.$$

Thus, these are all distinct modulo n.

We now must show $x = x_0 + \frac{n}{d}t$ is congruent to

one of the above. Use the Division alg to write

$$t = qd + r \qquad 0 \le r \le d-1.$$

Then,
$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd+r) \\ &= x_0 + nd + \frac{nr}{d} \\ &\equiv x_0 + \frac{n}{d}r \pmod{n}. \end{aligned}$$

■

<u>Example</u>: Solve the linear congruence

$$34x \equiv 60 \pmod{98}.$$

<u>Solution</u>: Begin by observing that $\gcd(34, 98) = 2$ and $2 \mid 60$ so there are solutions. In fact, we have exactly 2 incongruent solutions modulo 98. Solutions are equivalent to solutions of the Diophantine problem

$$34x - 60 = 98y$$

i.e.,

$$34x + 98y = 60$$

where we replaced $-y$ with y (since we are only interested in x this won't affect us!) Since $\gcd(34, 98) = 2$, we can find m, n so that

$$34m + 98n = 2.$$

$m = -23$, $n = 8$

Thus, $$34(-23) + 98(8) = 2.$$

Multiplying by 30 we have

$$34(-690) + 98(240) = 60$$

Thus, $x = -690$ is one solution.

Note that .

Example: Solve the linear congruence

$$34x \equiv 60 \pmod{98}.$$

Solution: Begin by observing that $\gcd(34, 98) = 2$ and $2 \mid 60$ so there are solutions. In fact, we have exactly 2 incongruent solutions modulo 98. Solutions are equivalent to solution of the Diophantine problem

$$34x - 60 = 98y$$

i.e.,

$$34x + 98y = 60$$

where we replaced $-y$ with y (since we are only interested in x this won't affect us!) Since $\gcd(34, 98) = 2$, we can find m, n so that

$$34m + 98n = 2.$$

$m = -23$, $n = 8$

Thus, $34(-23) + 98(8) = 2$.

Multiplying by 30 we have

$$34(-690) + 98(240) = 60$$

Thus, $x = -690$ is one solution.

Note that ~~[illegible]~~.

$$-690 \equiv 94 \pmod{98}$$

Thus, $x = 94$ is one solution to the equation. The other solution is

$$94 + \frac{98}{2} = 143$$

$\frac{n}{d}$

$$\equiv 45 \pmod{98}.$$

Thus, our two incongruent solution are 45 and 94.

The next natural step is to try and solve two congruences

$$a_1 x \equiv b_1 \pmod{m_1}$$
$$a_2 x \equiv b_2 \pmod{m_2}$$

$\gcd(m_1, m_2) = 1.$

simultaneously. Each equation only has a solution if $\gcd(m_i, a_i) \mid b_i$. If this is the case, divide by $d_i = \gcd(m_i, a_i)$ to obtain new equations

$$\frac{a_1}{d_1} x \equiv \frac{b_1}{d_1} \pmod{\frac{m_1}{d_1}}$$

$$\frac{a_2}{d_2} x \equiv \frac{b_2}{d_2} \pmod{\frac{m_2}{d_2}}.$$

Each of these equations has a solution, say

$x \equiv c_1 \pmod{\frac{m_1}{d_1}}$ and

$$X \equiv c_2 \pmod{\frac{m_2}{d_2}}.$$

Now we want to determine which of these solutions solve both of the congruences simultaneously. Thus, we have reduced solving

$$a_1 x \equiv b_1 \pmod{m_1}$$
$$a_2 x \equiv b_2 \pmod{m_2}$$

simultaneously down to the problem of solving

$$X \equiv c_1 \pmod{\frac{m_1}{d_1}}$$
$$X \equiv c_2 \pmod{\frac{m_2}{d_2}}$$

simultaneously.

<u>Thm 4.8 (The Chinese Remainder Theorem):</u> Let n_1, n_2 be positive integers w/ $\gcd(n_1, n_2) = 1$. Then

$$X \equiv a_1 \pmod{n_1}$$
$$X \equiv a_2 \pmod{n_2}$$

has a simultaneous solution which is unique modulo $n_1 n_2$.

<u>Proof:</u> Let X be a solution of the equation

$$X \equiv a_1 \pmod{n_1}.$$

Then $\exists\, y \in \mathbb{Z}$ s.t.

$$x - a_1 = n_1 y$$

i.e.,

$$x = a_1 + n_1 y.$$

Putting this into the second equation we have

$$a_1 + n_1 y \equiv a_2 \pmod{n_2},$$

i.e., we want to solve the congruence

$$n_1 y \equiv (a_2 - a_1) \pmod{n_2}.$$

Since $\gcd(n_1, n_2) = 1$, this equation has a solution. Write

$$n_1 s + n_2 t = 1.$$

Then

$$n_1 s(a_2 - a_1) + n_2 t(a_2 - a_1) = a_2 - a_1$$

i.e,

$$n_1 (s(a_2 - a_1)) \equiv a_2 - a_1 \pmod{n_2}.$$

So letting

$$x = a_1 + n_1 s(a_2 - a_1)$$

we see that

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

and

$$\begin{aligned} x &\equiv a_1 + n_1 s(a_2 - a_1) \\ &\equiv a_1 + (a_2 - a_1) \pmod{n_2} \\ &\equiv a_2 \pmod{n_2}. \end{aligned}$$

Thus, x is a solution simultaneously to each congruence. Now observe that if x' is another simultaneous solution, then

$$x \equiv x' \pmod{n_1}$$
$$x \equiv x' \pmod{n_2}.$$

Since $n_1 \mid (x-x')$ and $n_2 \mid (x-x')$, $\operatorname{lcm}(n_1, n_2) \mid (x-x')$. However, $\gcd(n_1, n_2) = 1 \Rightarrow \operatorname{lcm}(n_1, n_2) = n_1 n_2$, thus, $n_1 n_2 \mid (x-x')$, ie., $x \equiv x' \pmod{n_1 n_2}$. Thus x is the unique solution modulo $n_1 n_2$. ▣

It may occur that we want a simultaneous solution to several equations. We can just apply the above theorem to find solutions in pairs. You'll prove this in your homework, but now we give an example.

Example: Solve the simultaneous congruences

$$x \equiv 5 \pmod{11}, \quad x \equiv 14 \pmod{29}, \quad x \equiv 15 \pmod{31}.$$

Solution: We first find a simultaneous solution to the congruences

$$x \equiv 5 \pmod{11}$$
$$x \equiv 14 \pmod{29}.$$

Write $x - 5 = 11y$, i.e, $x = 5 + 11y$.

Substituting this into the second equation gives

$$5 + 11y \equiv 14 \pmod{29}.$$

i.e, $$11y \equiv 9 \pmod{29}.$$

Next we need ~~[illegible]~~ $s, t \in \mathbb{Z}$

s.t. $$11s + 29t = 1.$$

We find $s = 8$, $t = -3$. Multiplying by 9 we have $11(72) + 29(-27) = 9$. Thus,

$11(72) \equiv 9 \pmod{29}$

Substituting back in we obtain

$$x = 5 + 11(72) = 797$$
$$\equiv 159 \pmod{319}$$

is a solution to the first pair of congruences. To find a solution to all three congruences is now equivalent to solving the congruences

$$X \equiv 159 \pmod{319}$$

$$x \equiv 15 \pmod{31}.$$

Write

$$X = 159 + 319z$$

and substitute into the second equation:

$$159 + 319z \equiv 15 \pmod{31}$$

i.e,

$$9z \equiv 11 \pmod{31}.$$

We now find $m, n \in \mathbb{Z}$ s.t $9m + 31n = 1$.

We have

$$1 = 9(7) + 31(-2)$$

Multiplying by 11:

$$11 = 9(77) + 31(-22).$$

i.e,

$$9(77) \equiv 11 \pmod{31}.$$

Thus,

$$X = 159 + 319(77)$$

$$= 24722$$
$$\equiv 4944 \ (9889).$$

Thus, $x = 4944 \pmod{9889}$ is a simultaneous solution, as you can check.

If you want to solve a system with SAGE, say

$$x \equiv a \pmod{m},$$
$$x \equiv b \pmod{n},$$

the command is

```
x = crt(a, b, m, n); x.
```

For example,

```
x = crt(5, 14, 11, 29); x
```

returns

797.

The text also treats solving

$$ax + by \equiv c \pmod{n}$$

as well as the simultaneous congruences

$$ax + by \equiv r \pmod n$$

$$cx + dy \equiv s \pmod n\ ,$$

but we will leave this for the reader to work out. It is not difficult and uses the same ideas we have been using.

Next we may ask about solving congruence of higher degrees, say

$$f(x) \equiv 0 \pmod n$$

for $f(x)$ a polynomial of degree r. We will deal with polynomials of degree 2 when we get to quadratic reciprocity. As in the case over $\mathbb{Z}$, there is not a nice easy way in general. The advantage to congruences is we can always solve them, just plug in $x = 0, \ldots, n-1$ and see which work. Of course, as n gets large this is not real efficient.

We can get a partial result. Suppose we want to solve

$$f(x) \equiv 0 \pmod{p^{n+1}}$$

for p a prime. We will see how we can use the solutions modulo p^n to get the solutions modulo p^{n+1}. This allows us to start modulo p and work our way up. So if we are going to do it computationally, this reduces our computations significantly. Also, if $m = p_1^{e_1} \cdots p_r^{e_r}$, then x is a solution of $f(x) \equiv 0 \pmod{m}$ iff $f(x) \equiv 0 \pmod{p_i^{e_i}}$ for each $i = 1, \ldots, r$. Thus we can at least reduce the problem down to studying equations modulo p.

We begin by observing that if x is s.t. $f(x) \equiv 0 \pmod{p^n}$, then $f(x) \equiv 0 \pmod{p^k}$ $\forall$ $1 \le k \le n$. Clearly if $p^n \mid f(x)$, so does p^k ~~[illegible]~~, for $1 \le k \le n$. Thus, if x is a solution of $f(x) \equiv 0 \pmod{p^{n+1}}$, x is also a solution of $f(x) \equiv 0 \pmod{p^n}$, which we are assuming we know all of. Let $x_1, \ldots, x_m$ be all of the solutions of $f(x) \equiv 0 \pmod{p^n}$. So we must have $x \equiv x_i \pmod{p^n}$ for some $i \in \{1, \ldots, m\}$. ~~We~~ ~~[illegible]~~ i.e, $\exists$ $t \in \mathbb{Z}$ s.t. $x - x_i = p^n t$, or $x = x_i + p^n t$. We want to determine for which i's such a t exists to make $x_i + p^n t$ a solution modulo p^{n+1}.

We have the following theorem giving the result:

If $p \mid f'(x_i)$ and $p^{n+1} \nmid f(x_i)$, then we get there are no solutions, again using our work on linear congruences.

If $p \mid f'(x_i)$ and $p^{n+1} \mid f(x_i)$, then $\gcd(p, f'(x_i)) = p \mid \left(\frac{f(x_i)}{p^n}\right)$ and so our work in linear congruences gives p solutions. ☒

<u>Example:</u> Find all solutions of the congruence

$$x^3 + 2x + 2 \equiv 0 \pmod{49}.$$

<u>Solution:</u> As $49 = 7^2$, we begin by solving the congruence

$$x^3 + 2x + 2 \equiv 0 \pmod{7}.$$

This is easy to calculate with substitutions, obtaining $x_1 \equiv 2$, $x_2 \equiv 3 \pmod{7}$.

$$f'(x) = 3x^2 + 2$$

So we want solutions of

$$t\, f'(x_i) \equiv -\frac{f(x_i)}{7} \pmod{7}.$$

The two values of x_i give:

$$t\,(0) \equiv -\frac{14}{7} \pmod{7}.$$

Thus $p \mid f'(2)$ and $p^2 \nmid f(2)$, so we have no solution corresponding to $x_1 = 2$.

$$f'(3) = 1 \pmod{7}$$

$$f(3) = 0 \pmod{7}, \quad f(3) = 35.$$

Thm: Let f be a polynomial with integer coefficients of degree $r \geq 1$. Let p be prime, $n \geq 1$. Let y be a solution of

$$f(x) \equiv 0 \pmod{p^{n+1}}.$$

Then $y = x_i + tp^n \pmod{p^{n+1}}$ where $0 \leq x_i \leq p^n$ and x_i satisfies

$$f(x_i) \equiv 0 \pmod{p^n}.$$

s.t $0 \leq t \leq p-1$ and t satisfies the congruence

$$t f'(x_i) \equiv \frac{-f(x_i)}{p^n} \pmod{p}. \qquad (*)$$

Furthermore, if h is the number of solutions of $(*)$, then

$$h = \begin{cases} 1 & \text{if } p \nmid f'(x_i) \\ 0 & \text{if } p \mid f'(x_i) \text{ and } p^{n+1} \nmid f'(x_i) \\ p & \text{if } p \mid f'(x_i) \text{ and } p^{n+1} \mid f'(x_i). \end{cases}$$

Proof: Let $x_1, \ldots, x_m$ be the solutions to $f(x) \equiv 0 \pmod{p^n}$.

~~Let~~ If $f(y) \equiv 0 \pmod{p^{n+1}}$, then $\exists\, i \in \{1, \ldots, m\}$ and $t \in \{0, \ldots, p-1\}$ s.t $y = x_i + tp^n$.

We consider the polynomial

$$f(y) = f(x_i + tp^n)$$

and expand it in a Taylor series. For ease, write

$$f(y) = f(x_i + x)$$

and the Taylor series around x_i is:

$$f(y) = f(x_i) + (y-x_i)f'(x_i) + \frac{(y-x_i)^2}{2} f''(x_i) + \cdots$$

$$= f(x_i) + x f'(x_i) + \frac{x^2}{2} f''(x_i) + \cdots$$

$$= f(x_i) + t p^n f'(x_i) + \frac{t^2 p^{2n}}{2} f''(x_i) + \cdots$$

Looking at this modulo p^{n+1} we have

$$f(y) \equiv f(x_i) + t p^n f'(x_i) \pmod{p^{n+1}}.$$

We have $f(y) \equiv 0 \pmod{p^{n+1}}$ by assumption, so

$$t p^n f'(x_i) \equiv -f(x_i) \pmod{p^{n+1}}.$$

We know $f(x_i) \equiv 0 \pmod{p^n}$, so $p^n \mid f(x_i)$. So we have $t p^n f'(x_i) + f(x_i) = s p^{n+1}$ and

$$f(x_i) = p^n l.$$

Thus,

$$t p^n f'(x_i) + p^n l = s p^{n+1}, \text{ i.e.,}$$

$$t f'(x_i) + l = s p.$$

Hence

$$t f'(x_i) \equiv -\frac{f(x_i)}{p^n} \pmod{p}.$$

This gives the first part of the theorem.

Let h be the number of solutions of $(*)$.

If $p \nmid f'(x_i)$, then this is a linear congruence and $\gcd(p, f'(x_i)) = 1$, so it has exactly 1 solution.

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

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

Thus, we obtain one solution (as we should since $7 \nmid f'(3)$)

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

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.

<u>Thm 5.1:</u> (Fermat's little theorem) Let p be a prime. 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.

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