Homework 1

Rebekah Mayne
Math 370, Fall 2024

February 13, 2025

1 (Page 19)

Problem 12. Let p be the least prime factor of n, where n is composite. Prove that if $p > n^{1/3}$, then n/p is prime.

Proof.
Let p be the least prime factor of n, where n is composite, meaning in this case $p < n$. Let $p > n^{1/3}$. We know that $p \cdot k = n$ for some k, assume to the contrary that k is composite, so $\exists\, m_1, m_2 \in \mathbb{Z}$ s.t. $m_1 \cdot m_2 = k$. Then, we have that $p \cdot m_1 \cdot m_2 = n$. We also know that $m_1, m_2 < p$ since p is the least prime factor. So we have that

$$\begin{aligned} p \cdot m_1 \cdot m_2 &> p^3 \\ p \cdot m_1 \cdot m_2 &> p^3 > \left[n^{1/3}\right]^3 \\ p \cdot m_1 \cdot m_2 &> n \\ n &> n \end{aligned}$$

But this is an obvious contradiction, so we know that k must be prime, and by our definition $k = {}^{n}/_{p}$ so we know that ${}^{n}/_{p}$ is prime. ☐

Problem 14. Prove that if n is composite. then $2^n - 1$ is composite.

Proof.
Let n be composite, so $\exists\, p, q$ s.t. $p \cdot q = n$ Let $m = 2^p - 1$, and lets look at this $\pmod m$,

$$\begin{aligned} 2^p - 1 &\pmod m \equiv 0 \\ 2^p &\pmod m \equiv 1 \\ (2^p)^q &\pmod m \equiv 1 \\ (2^p)^q - 1 &\pmod m \equiv 0 \end{aligned}$$

This can be rewritten as $m | \left(2^{pq} - 1\right)$, or $m | \left(2^n - 1\right)$ which means that $2^n - 1$ is composite as well. ☐

Problem 15. Is it true that if $2^n - 1$ is composite, then n is composite?

Solution.

Let p be a divisor of $2^n - 1$, this means that

$$2^n - 1 \equiv 0 \pmod{p}$$
$$2^n \equiv 1 \pmod{p}$$

We can see that this means that 2 is it's own inverse in $\mod p$, so if n was odd $2^n \equiv 2 \pmod{p}$, but since $2^n \equiv 1 \pmod{p}$ we know that n must be even. This means that n is either composite, or $n = 2$, so it is nt always true, but if $n \neq 2$ then it is.

2

Problem . Find the smallest positive integer n such that $15120n$ is a perfect square. (**Hint:** How could you identify a perfect square if you were able to see its PPF?)

Solution.

First we want to find the PPF of 15120, we can find that as follows,

$$\begin{aligned} &15120 \\ &\qquad 15120 \equiv 0 \pmod{5} \\ 15120 = {}& 5 \cdot 3024 \\ &\qquad 3024 \equiv 0 \pmod{4} \\ 15120 = {}& 5 \cdot 2^2 \cdot 756 \\ &\qquad 756 \equiv 0 \pmod{4} \\ 15120 = {}& 5 \cdot 2^4 \cdot 189 \\ &\qquad 189 \equiv 0 \pmod{9} \\ 15120 = {}& 5 \cdot 2^4 \cdot 3^2 \cdot 21 \end{aligned}$$

So the PPF is $2^4 \cdot 3^3 \cdot 5 \cdot 7$, the smallest n that would make $2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot n$ a perfect square would be $n = 3 \cdot 5 \cdot 7$ or $n = 105$.

This would make $15120n = 1589600$, which is 1260^2.

---

3 (Page 26)

Problem 4. Find all the solutions in positive integers of $2x+y = 2$, $3x-4y = 0$, and $7x+15y = 51$.

Solution.

(a) $2x + y = 2$
One solution we can see by inspection is $x = 2$ and $y = -2$. Then, all solutions will be

$$x = 2 + \frac{1}{(1,2)}t \qquad\qquad y = -2 + \frac{2}{(1,2)}t$$
$$x = 2 + t \qquad\qquad y = -2 + 2t$$

(b) $3x - 4y = 0$
One solution we can see by inspection is $x = 4$ and $y = -3$. Then, all solutions will be

$$x = 4 + \frac{4}{(3,4)}t \qquad\qquad y = -3 + \frac{3}{(3,4)}t$$
$$x = 4 + 4t \qquad\qquad y = -3 + 3t$$

(c) $7x + 15y = 51$
One solution we can see by inspection of $7x + 15y = 1$ would be $x = 2$ and $y = -1$, so one solution to $7x + 15y = 51$ would be $x = 102$ and $y = -51$. Then, all solutions will be

$$x = 102 + \frac{15}{(7,15)}t \qquad\qquad y = -51 + \frac{7}{(7,15)}t$$
$$x = 102 + 15t \qquad\qquad y = -51 + 7t$$

---

4 (Pages 32 - 33)

Problem 2. Find the least residue of $1789 \pmod 4$, $\pmod{10}$, and $\pmod{101}$.

Solution.

- $1789 \pmod 4$

$$\begin{aligned} 1789 &= 1600 + 189 \\ 1789 &\equiv 0 + 160 + 29 \pmod 4 \\ 1789 &\equiv 0 + 0 + 28 + 1 \pmod 4 \\ 1789 &\equiv 1 \pmod 4 \end{aligned}$$

- $1789 \pmod{10}$

$$\begin{aligned} 1789 &= 1700 + 89 \\ 1789 &\equiv 0 + 80 + 9 \pmod{10} \\ 1789 &\equiv 9 \pmod{10} \end{aligned}$$

- $1789 \pmod{101}$

$$\begin{aligned}
1789 &= 1717 + 72 \\
1789 &\equiv 0 + 72 && \pmod{101} \\
1789 &\equiv 72 && \pmod{101}
\end{aligned}$$

Problem 6. Find all m such that $1848 \equiv 1914 \pmod{m}$.

Solution.

$1848 \equiv 1914 \pmod{m}$ iff $1914 = 1848 + km$ for some $k \in \mathbb{Z}$. This means that we need $66 = km$. The PPD of 66 is $11 \cdot 3 \cdot 2$, so m can be in $\{2, 3, 6, 11, 22, 33, 66\}$.

Problem 8. Show that every prime (except 2) is congruent to 1 or $3 \pmod{4}$.

Proof.

Let p be any prime (other than 2). By definition we know that $2 \nmid p$. We also can see that for $a \equiv 2 \pmod{4}$ or $a \equiv 0 \pmod{4}$ that either $a = 2 + 4k$ or $a = 4k$ for some k. No matter what k we choose, $2|4k$, so $2|a$ must also be true. Therefore we know that $p \neq a$, so p must be congruent to either 1 or $3 \pmod{4}$. $\square$

Problem 9. Show that every prime (except 2 or 3) is congruent to 1 or $5 \pmod{6}$.

Proof.

Let p be any prime (other than 2 or 3). By definition $2 \nmid a$ and $3 \nmid a$. For a to be congruent to 2, 3, 4, or 0, then one of the following must be true: $a = 6k$, $a = 2 + 6k$, $a = 3 + 6k$, or $a = 4 + 6k$. Then we can see that either $2|a$ ($a = 6k$, $a = 2 + 6k$, or $a = 4 + 6k$), or $3|a$ ($a = 6k$ or $a = 3 + 6k$). Therefore $a \neq p$. So p must be congruent to 1 or $5 \pmod{6}$. $\square$

Problem 10. What can primes (except 2,3, or 5) be congruent to $\pmod{30}$?

Solution.

Let p be any prime (other than 2,3, or 5). Then, p must be congruent to a where $a \neq k$ for $k \perp 30$. So p must be congruent to something in the set $\{1, 7, 11, 13, 17, 19, 23, 29\}$.

Problem 11. In the multiplication $31415 \cdot 92653 = 2910\_93995$, one digit in the product is missing and all the others are correct. Find the missing digit without doing the multiplication.

Solution.

We can see that $11|92653$ by the 11 division prop, because $9 - 2 + 6 - 5 + 3 = 11$. This means that we know that our answer must also be divisible by 11. Subbing in x for our missing digit we can get that

$$2 + 9 - 1 + 0 - x + 9 - 3 + 9 - 9 + 5 = 21 - x$$

For $21 - x \equiv 0 \pmod{11}$ and $0 \leq x \leq 9$, we see that $x = 9$. So our mising digit is 9.

Problem 14. Show that the difference of two consecutive cubes is never divisible by 3.

Proof.
Let $x = a^3$ and $y = (a+1)^3$. Then

$$\begin{aligned} y - x &= (a+1)^3 - a^3 \\ &= a^3 - 3a^2 + 3a - 1 - a^3 \\ &= -3a^2 + 3a - 1 \\ &\equiv -1 \pmod 3 \end{aligned}$$

This means that the difference two consecutive cubes will always be equivalent to -1 mod 3. □

Problem 15. Show that the difference of two consecutive cubes is never divisible by 5.

Proof.
Let $x = a^3$ and $y = (a+1)^3$. Then

$$\begin{aligned} y - x &= (a+1)^3 - a^3 \\ &= a^3 - 3a^2 + 3a - 1 - a^3 \\ &= -3a^2 + 3a - 1 \\ &\equiv -3a^2 + 3a - 1 \pmod 5 \end{aligned}$$

Assume to the contrary that it is divisible by 5, then

$$\begin{aligned} -3a^2 + 3a - 1 &\equiv 0 \pmod 5 \\ -3a^2 + 3a &\equiv 1 \pmod 5 \\ -3(a^2 - a) &\equiv 1 \pmod 5 \\ 2(a^2 - a) &\equiv 1 \pmod 5 \end{aligned}$$

Then we can make the chart:

$a \pmod 5$	$0 \pmod 5$	$1 \pmod 5$	$2 \pmod 5$	$3 \pmod 5$	$4 \pmod 5$
$a^2 \pmod 5$	0	1	4	$9 \equiv 4$	$16 \equiv 1$
$a^2 - a \pmod 5$	0	0	2	1	$-3 \equiv 2$
$2(a^2 - a) \pmod 5$	0	0	4	2	4

We can see that none of these are able to be congruent to 1, so we can see that this is a contradiction so the difference of two consecutive cubes is never divisible by 5.

□

Problem 19. Show that if $n \equiv 4 \pmod 9$, then n cannot be written as the sum of three cubes.

Solution.
We can make the chart:

$r \pmod 9$	0	1	2	3	4	5	6	7	8
$r^2 \pmod 9$	0	1	4	0	7	7	0	4	1
$r^3 \pmod 9$	0	1	8	0	1	8	0	1	8

We can see that cubes can only be congruent to 0, 1 or 8 in mod 9. So the only sums that three cubes can get to are 0, 1, 2, 3, 8, $9 \equiv 0$, $10 \equiv 1$, $16 \equiv 5$, $17 \equiv 6$, or $24 \equiv 6$. So there is no way for the sum of three cubes to be congruent to 4 mod 9.

---

5 (Pages 40 - 41)

Problem 1. Solve each of the following:

(a) $2x \equiv 1 \pmod{17}$

(b) $3x \equiv 1 \pmod{17}$

(c) $3x \equiv 6 \pmod{18}$

(d) $40x \equiv 777 \pmod{1777}$

Solution.

(a) $(2, 17) = 1$, so there is only 1 solution and it is $x \equiv 9 \pmod{17}$.

(b) Since $(3, 17) = 1$, there is only 1 solution and it is $x \equiv 6 \pmod{17}$.

(c) Since $(3, 18) = 3$, and $3|6$, we can rewrite it as $x \equiv 2 \pmod 6$. Then, there are 3 solutions, and they are $x \equiv 2, 8, 14 \pmod{18}$.

(d) $(40, 1777) = 1$, so there is only 1 solution, and we can use EA to solve as follows,

$$\begin{aligned}
1777 &= 40(44) + 17 \\
40 &= 17(2) + 6 \\
17 &= 6(2) + 5 \\
6 &= 5(1) + 1 \\
5 &= 1(5) + 0
\end{aligned}$$

Then using back substitution,

$$\begin{aligned}
1 &= 6 - 5 \\
&= 6 - 17 + 6(2) \\
&= 17(-1) + 6(3) \\
&= 17(-1) + 3(40 - 17(2)) \\
&= 17(-1) + 40(3) + 17(-6) \\
&= 17(-7) + 40(3) \\
&= (-7)(1777 - 40(44)) + 40(3) \\
&= 1777(-7) + 40(308) + 40(3) \\
1 &= 1777(-7) + 40(311) \\
777 &= 1777(-5439) + 40(241647) \\
777 &= 40(241647) \pmod{1777} \\
777 &= 40(1752) \pmod{1777}
\end{aligned}$$

So we can see that $x \equiv 1752 \pmod{1777}$

Problem 3. Solve the systems

(a) $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$.

(b) $x \equiv 3 \pmod 5$, $x \equiv 5 \pmod 7$, $x \equiv 7 \pmod{11}$.

(c) $2x \equiv 1 \pmod 5$, $3x \equiv 2 \pmod 7$, $4x \equiv 3 \pmod{11}$.

Solution.

(a) Let $k_1, k_2 \in \mathbb{Z}$. Then we can do the following,

$$\begin{array}{lll}
x \equiv 1 \pmod 2 & \rightarrow & x = 2k_1 + 1 \\
2k_1 + 1 \equiv 1 \pmod 3 & \leftarrow & \\
2k_1 \equiv 0 \pmod 3 & & \\
k_1 \equiv 0 \pmod 3 & \rightarrow & k_1 = 3k_2 \\
 & & x = 2(3(k_2)) + 1 \\
 & & x = 6k_2 + 1 \\
x \equiv 1 \pmod 6 & \leftarrow &
\end{array}$$

(b) Let $k_1, k_2, k_3 \in \mathbb{Z}$. Then we can do the following,

$$\begin{array}{lll}
x \equiv 3 \pmod 5 & \rightarrow & x = 5k_1 + 3 \\
5k_1 + 3 \equiv 5 \pmod 7 & \leftarrow & \\
5k_1 \equiv 2 \pmod 7 & & \\
k_1 \equiv 6 \pmod 7 & \rightarrow & k_1 = 7k_2 + 6 \\
 & & x = 5(7k_2 + 3) + 6 \\
 & & x = 35k_2 + 15 + 6 \\
 & & x = 35k_2 + 21 \\
35k_2 + 21 \equiv 7 \pmod{11} & \leftarrow & \\
2k_2 - 1 \equiv 7 \pmod{11} & & \\
2k_2 \equiv 8 \pmod{11} & & \\
k_2 \equiv 4 \pmod{11} & \rightarrow & k_2 = 11k_3 + 4 \\
 & & x = 35(11k_3 + 4) + 21 \\
 & & x = 385k_3 + 140 + 21 \\
 & & x = 385k_3 + 161 \\
x \equiv 161 \pmod{385} & \leftarrow &
\end{array} \qquad [l]$$

(c) [(b)] Let $k_1, k_2, k_3 \in \mathbb{Z}$. Then we can do the following,

$$\begin{array}{lll}
2x \equiv 1 \pmod 5 & & \\
x \equiv 3 \pmod 5 & \rightarrow & x = 5k_1 + 3 \\
3(5k_1 + 3) \equiv 2 \pmod 7 & \leftarrow & \\
15k_1 + 9 \equiv 2 \pmod 7 & & \\
k_1 \equiv 0 \pmod 7 & \rightarrow & k_1 = 7k_2 \\
 & & x = 5(7k_2) + 3 \\
 & & x = 35k_2 + 3 \\
4(35k_2 + 3) \equiv 3 \pmod{11} & \leftarrow & \\
k_2 + 1 \equiv 3 \pmod{11} & & \\
k_2 \equiv 2 \pmod{11} & \rightarrow & k_2 = 11k_3 + 2 \\
 & & x = 35(11k_3 + 2) \\
 & & x = 385k_3 + 70 \\
x \equiv 70 \pmod{385} & \leftarrow &
\end{array}$$

Problem 5. What possibilities are there for number of solutions of a linear congruence (mod 20)

Solution.

The possibilities are any possibilities of $(a, 20)$, which can be anything in the set $\{0, 1, 2, 4, 5, 10, 20\}$

Problem 6. Construct linear congruences modulo 20 with no solutions, just one solution, and more than one solution. Can you find one with 20 solutions?

Solution.

No Solutions:

$$ax \equiv b \pmod{20} \qquad \text{where } (a, m) \nmid b$$

Ex:

$$5x \equiv 7 \pmod{20}$$

1 Solutions:

$$ax \equiv b \pmod{20} \qquad \text{where } (a, m) = 1$$

Ex:

$$7x \equiv 13 \pmod{20} \rightarrow \quad x \equiv 19 \pmod{20}$$

k Solutions:

$$ax \equiv b \pmod{20} \qquad \text{where } (a, m) = k \text{ and } k|b$$

Ex (2):

$$6x \equiv 14 \pmod{20} \rightarrow \quad x \equiv 9, 19 \pmod{20}$$

Ex (4):

$$8x \equiv 16 \pmod{20} \rightarrow \quad x \equiv 2, 6, 10, 16 \pmod{20}$$

Ex (5):

$$15x \equiv 5 \pmod{20} \rightarrow \quad x \equiv 3, 7, 11, 15, 19 \pmod{20}$$

Ex (10):

$$10x \equiv 10 \pmod{20} \rightarrow \quad x \equiv 1, 3, 5, 7, 9, 11, 13, 15, 17, 19 \pmod{20}$$

Ex (20):

$$\begin{aligned} 20x \equiv 20 \pmod{20} \rightarrow \quad x \equiv\ & 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 \\ & 12, 13, 14, 15, 16, 17, 18, 19 \pmod{20} \end{aligned}$$

6

Problem . Let $f(x) = x^2 + x + 41$.

(a) Have Sage compute $f(n)$ for $n = 1, 2, \cdots, 10$ and make a conjecture about the possible values of $f(n)$ when n is any positive integer

(b) Prove or disprove your conjecture from part (a).

(c) **Extra Credit:** Prove that for any polynomial of the form $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and $a \neq 0$, $f(n)$ will be *composite* for infinitely many positive integers n.

(d) **Extra Credit:** Prove that you can find a non-constant quadratic polynomial $f(x)$ such that $f(n)$ is prime for infinitely many values of n. (**Hint:** Do the rest of your homework first)

Solution.

(a)

```
def f(x):
    return x^2+x+41

def prime_check(a):
    if a.is_prime() == True:
        return "Prime"
```

```
    else:
        return "Composite"

print(f'The solutions for f(x) when x is between 1 and 10 are as follows')

for a in range(1,11):
    answer = f(a)
    a_prime = prime_check(answer)
    if a< 10:
        if answer<100:
            print(f'x={a}  : f(x)={answer}  |{answer}  is {a_prime}')
        else:
            print(f'x={a}  : f(x)={answer} |{answer} is {a_prime}')

    else:
        if answer<100:
            print(f'x={a} : f(x)={answer}  |{answer}  is {a_prime}')
        else:
            print(f'x={a} : f(x)={answer} |{answer} is {a_prime}')
```

```
    The solutions for f(x) when x is between 1 and 10 are as follows
    x=1  : f(x)=43  |43  is Prime
    x=2  : f(x)=47  |47  is Prime
    x=3  : f(x)=53  |53  is Prime
    x=4  : f(x)=61  |61  is Prime
    x=5  : f(x)=71  |71  is Prime
    x=6  : f(x)=83  |83  is Prime
    x=7  : f(x)=97  |97  is Prime
    x=8  : f(x)=113 |113 is Prime
    x=9  : f(x)=131 |131 is Prime
    x=10 : f(x)=151 |151 is Prime
```

My conjecture is that $f(n)$ will be prime for all n.

(b)

```
def f(x):
    return x^2+x+41

upper = 100

for a in range(1,upper+1):
    an = f(a)
    if an.is_prime() == False:
        counter = an
        break
    else:
        counter = "none"
        continue

if counter == "none":
    print(f'There are no f(x) that are composite up to f({a}).')
else:
    print(f'There is f({a})={counter} that is composite.')
```

```
    There is f(40)=1681 that is composite.
```

(c) Let $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and $a \neq 0$. Assume for contradiction that $f(n)$ for all

n be prime. Then let $n = c$. Then we can see

$$\begin{aligned} f(c) &= a(c)^2 + b(c) + c \\ &\equiv ac^2 + b(c) + c \pmod{c} \\ &\equiv 0 \pmod{c} \end{aligned}$$

By definition this means that $f(c) = c \cdot k$ for some k but this means that $c|f(c)$, which means that $f(c)$ is not prime, so this is a contradiction. We can also see that this will be true for any $f(n)$ where $c|n$.

So we can see that $f(n)$ will be composite for infinitely many positive integers n.

(d)