Homework 4

Rebekah Mayne
Math 370, Fall 2024

May 9, 2025

1 (Page 93)

Problem 2. Which of the following congruences have solutions?

$$\begin{array}{llll} a) & x^2 \equiv 8 \pmod{53} & b) & x^2 \equiv 15 \pmod{31} \\ c) & x^2 \equiv 54 \pmod{7} & d) & x^2 \equiv 625 \pmod{9973} \end{array}$$

Solution.

a) **No Solution**

$$\begin{aligned} 8^{\frac{53-1}{2}} &\equiv 8^{26} &\pmod{53} \\ &\equiv (8^2)^13 &\pmod{53} \\ &\equiv (11)^13 &\pmod{53} \\ &\equiv 11 \cdot (11^3)^4 &\pmod{53} \\ &\equiv 11 \cdot (6)^4 &\pmod{53} \\ &\equiv 11 \cdot 6 \cdot 4 &\pmod{53} \\ &\equiv 44 \cdot 6 &\pmod{53} \\ &\equiv -9 \cdot 6 &\pmod{53} \\ &\equiv -54 &\pmod{53} \\ &\equiv -1 &\pmod{53} \end{aligned}$$

b) **No Solution**

$$\begin{aligned} 15^{\frac{31-1}{2}} &\equiv 15^{15} &\pmod{31} \\ &\equiv (3375)^5 &\pmod{31} \\ &\equiv (3100 + 275)^5 &\pmod{31} \\ &\equiv (0 + 279 - 4)^5 &\pmod{31} \\ &\equiv (-4)^5 &\pmod{31} \\ &\equiv (-4)^2 \cdot (-4)^3 &\pmod{31} \\ &\equiv 16 \cdot -2 &\pmod{31} \\ &\equiv -32 &\pmod{31} \\ &\equiv -1 &\pmod{31} \end{aligned}$$

c) **No Solution**

$$\begin{aligned} 54^{\frac{7-1}{2}} &\equiv 5^3 &\pmod{7} \\ &\equiv 25 \cdot 5 &\pmod{7} \\ &\equiv -3 \cdot 5 &\pmod{7} \\ &\equiv -15 &\pmod{7} \\ &\equiv -1 &\pmod{7} \end{aligned}$$

d) **Has a Solution**

625 is a square already

Problem 4. Find solutions for the congruences in Problem 2 that have them.

Solution.

Looking at $x^2 \equiv 625 \pmod{9973}$, we can see that $625 = 26^2$ so $x = 25$ is the solution. Then the other solution is $-25 \pmod{9973} \equiv 9948$, so the solutions are, 25 and 9948.

Problem 5. Calculate $\left(\frac{33}{71}\right)$, $\left(\frac{34}{71}\right)$, $\left(\frac{35}{71}\right)$, and $\left(\frac{36}{71}\right)$.

Solution.

$$\begin{aligned}
\left(\tfrac{33}{71}\right) &= \left(\tfrac{3}{71}\right)\cdot\left(\tfrac{11}{71}\right)\\
&= (-1)\cdot\left(\tfrac{71}{3}\right)\cdot(-1)\cdot\left(\tfrac{71}{11}\right)\\
&= \left(\tfrac{2}{3}\right)\cdot\left(\tfrac{7}{11}\right)\\
&= -1\cdot\left(\tfrac{11}{7}\right)\\
&= -\left(\tfrac{4}{7}\right)\\
\left(\tfrac{33}{71}\right) &= -1
\end{aligned}$$

$$\begin{aligned}
\left(\tfrac{34}{71}\right) &= \left(\tfrac{2}{71}\right)\cdot\left(\tfrac{17}{71}\right)\\
&= 1\cdot(-1)\left(\tfrac{71}{17}\right)\\
&= -\left(\tfrac{3}{17}\right)\\
&= \left(\tfrac{17}{3}\right)\\
&= \left(\tfrac{2}{3}\right)\\
&= -1\\
\left(\tfrac{34}{71}\right) &= 1
\end{aligned}$$

$$\begin{aligned}
\left(\tfrac{35}{71}\right) &= \left(\tfrac{5}{71}\right)\cdot\left(\tfrac{7}{71}\right)\\
&= -1\cdot\left(\tfrac{71}{5}\right)\cdot\left(\tfrac{71}{7}\right)\\
&= -1\cdot\left(\tfrac{1}{5}\right)\cdot 17\\
\left(\tfrac{35}{71}\right) &= -1
\end{aligned}$$

$$\left(\tfrac{36}{71}\right) = 1 \quad {}^*(36 = 6^2)$$

Problem 6. Calculate $\left(\frac{33}{73}\right)$, $\left(\frac{34}{73}\right)$, $\left(\frac{35}{73}\right)$, and $\left(\frac{36}{73}\right)$.

Solution.

$$\begin{aligned}
\left(\tfrac{33}{73}\right) &= \left(\tfrac{11}{73}\right)\cdot\left(\tfrac{3}{73}\right)\\
&= \left(\tfrac{73}{11}\right)\cdot\left(\tfrac{73}{3}\right)\\
&= \left(\tfrac{7}{11}\right)\cdot\left(\tfrac{1}{3}\right)\\
&= -1\cdot\left(\tfrac{11}{7}\right)\\
&= -1\cdot\left(\tfrac{4}{7}\right)\\
\left(\tfrac{33}{73}\right) &= -1
\end{aligned}$$

$$\begin{aligned}
\left(\tfrac{34}{73}\right) &= \left(\tfrac{2}{73}\right)\cdot\left(\tfrac{17}{73}\right)\\
&= 1\cdot\left(\tfrac{73}{17}\right)\\
&= \left(\tfrac{5}{17}\right)\\
&= \left(\tfrac{17}{5}\right)\\
&= \left(\tfrac{2}{5}\right)\\
\left(\tfrac{34}{73}\right) &= -1
\end{aligned}$$

$$\begin{aligned}
\left(\tfrac{35}{73}\right) &= \left(\tfrac{5}{73}\right)\cdot\left(\tfrac{7}{73}\right)\\
&= \left(\tfrac{73}{5}\right)\cdot\left(\tfrac{73}{7}\right)\\
&= \left(\tfrac{3}{5}\right)\cdot\left(\tfrac{3}{7}\right)\\
&= \left(\tfrac{5}{3}\right)\cdot(-1)\cdot\left(\tfrac{7}{3}\right)\\
&= \left(\tfrac{2}{3}\right)\cdot(-1)\cdot\left(\tfrac{1}{3}\right)\\
&= (-1)\cdot(-1)\\
\left(\tfrac{35}{73}\right) &= 1
\end{aligned}$$

$$\left(\tfrac{36}{73}\right) = 1 \quad {}^*(36 = 6^2)$$

Problem 10. Calculate $\left(\frac{1356}{2467}\right)$ and $\left(\frac{6531}{2467}\right)$.

Solution.

First $1356 = 2^2 \cdot 3 \cdot 113$, and $2467 = 2400 + 60 + 4 + 3 \equiv 3 \pmod 4$, so we can start with

$$\begin{aligned}
\left(\frac{1356}{2467}\right) &= \left(\frac{2^2}{2467}\right) \cdot \left(\frac{3}{2467}\right) \cdot \left(\frac{113}{2467}\right) \\
&= (-1) \cdot \left(\frac{2467}{3}\right) \cdot \left(\frac{2467}{113}\right) \\
&= (-1) \cdot \left(\frac{1}{3}\right) \cdot \left(\frac{94}{113}\right) \\
&= (-1) \cdot \left(\frac{2}{113}\right) \cdot \left(\frac{47}{113}\right) \\
&= (-1) \cdot \left(\frac{113}{47}\right) \\
&= (-1) \cdot \left(\frac{19}{47}\right) \\
&= (-1) \cdot \left(\frac{47}{19}\right) \\
&= (-1) \cdot \left(\frac{9}{19}\right) \\
\left(\frac{1356}{2467}\right) &= -1
\end{aligned}$$

Then for the other, $6531 = 3 \cdot 7 \cdot 311$, and again $2467 \equiv 3 \pmod 4$, so we can start with

$$\begin{aligned}
\left(\frac{6531}{2467}\right) &= \left(\frac{3}{2467}\right) \cdot \left(\frac{7}{2467}\right) \cdot \left(\frac{311}{2467}\right) \\
&= (-1) \cdot \left(\frac{2467}{3}\right) \cdot (-1) \cdot \left(\frac{2467}{7}\right) \cdot (-1) \cdot \left(\frac{2467}{311}\right) \\
&= (-1) \cdot \left(\frac{1}{3}\right) \cdot \left(\frac{3}{7}\right) \cdot \left(\frac{290}{311}\right) \\
&= (-1) \cdot (-1) \left(\frac{7}{3}\right) \cdot \left(\frac{2}{311}\right) \cdot \left(\frac{5}{311}\right) \cdot \left(\frac{29}{311}\right) \\
&= \left(\frac{311}{5}\right) \cdot \left(\frac{311}{29}\right) \\
&= \left(\frac{1}{5}\right) \cdot \left(\frac{21}{29}\right) \\
&= \left(\frac{3}{29}\right) \cdot \left(\frac{7}{29}\right) \\
&= \left(\frac{29}{3}\right) \cdot \left(\frac{29}{7}\right) \\
&= \left(\frac{2}{3}\right) \cdot \left(\frac{1}{7}\right) \\
\left(\frac{6531}{2467}\right) &= -1
\end{aligned}$$

Problem 11. Show that if $p = q + 4a$ (p and q are odd primes), then $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$

Proof. Let p and q be odd primes such that $p = q + 4a$ (for some $a \in \mathbb{Z}$). Then look at

$$\begin{aligned}
\left(\frac{p}{q}\right) &= \left(\frac{q+4a}{q}\right) \\
&= \left(\frac{4a}{q}\right) \\
&= \left(\frac{4}{q}\right) \cdot \left(\frac{a}{q}\right) \\
&= 1 \cdot \left(\frac{a}{q}\right) \\
\left(\frac{p}{q}\right) &= \left(\frac{a}{q}\right)
\end{aligned}$$

□

Problem 16. Show that if a is a quadratic residue (mod p) and $ab \equiv 1 \pmod p$ then b is a quadratic residue (mod p).

Proof. Let a be a quadratic residue $\mod p$ and $ab \equiv 1 \pmod p$, then we know that $\left(\frac{a}{p}\right) = 1$, then we have

$$\begin{aligned}
\left(\frac{a}{p}\right) &= 1 \\
&= \left(\frac{1}{p}\right) \\
\left(\frac{a}{p}\right) &= \left(\frac{ab}{p}\right) \\
1 &= \left(\frac{ab}{p}\right) \\
1 &= \left(\frac{b}{p}\right) \cdot \left(\frac{a}{p}\right) \\
1 &= \left(\frac{b}{p}\right)
\end{aligned}$$

Which by definition means that b is also a quadratic residue (mod p). □

Problem 17. Does $x^2 \equiv 211 \pmod{159}$ have a solution? Note that 159 is not prime.

Solution.

Yes, since $221 \equiv 1 \pmod 3$, and $221 \equiv -1 \pmod{53}$ and $53 \equiv 1 \pmod 4$, so there should be solutions for $x^2 \equiv 211 \pmod 3$ and $x^2 \equiv 211 \pmod{53}$. Since $3 \perp 53$, there should be a solution for $x^2 \equiv 211 \pmod{159}$.

Problem 20. Suppose that $p = q + 4a$ where p and q are odd primes. Show that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Proof. Let p and q be odd primes, where $p = q + 4a$ for some $a \in \mathbb{Z}$. This means that $p \equiv q \pmod 4$, then there are two cases, one where it is equivalent to 1, and one where it is equivalent to 3.

If $p \equiv q \equiv 1 \pmod 4$, then

$$\begin{aligned}
\left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) \\
\left(\frac{q+4a}{q}\right) &= \left(\frac{p-4a}{p}\right) \\
\left(\frac{4a}{q}\right) &= \left(\frac{-4a}{p}\right) \\
\left(\frac{a}{q}\right) &= \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) \\
\left(\frac{a}{q}\right) &= \left(\frac{a}{p}\right)
\end{aligned}$$

If $p \equiv q \equiv 3 \pmod 4$, then

$$\begin{aligned}
\left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right) \\
\left(\frac{q+4a}{q}\right) &= -\left(\frac{p-4a}{p}\right) \\
\left(\frac{4a}{q}\right) &= -\left(\frac{-4a}{p}\right) \\
\left(\frac{a}{q}\right) &= -\left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) \\
\left(\frac{a}{q}\right) &= (-1) \cdot (-1) \cdot \left(\frac{a}{p}\right) \\
\left(\frac{a}{q}\right) &= \left(\frac{a}{p}\right)
\end{aligned}$$

We can see either way, this is true. □

---

2 pg 104

Problem 2. Show that 3 is a quadratic nonresidue of all Mersenne primes greater than 3.

Solution.

Let $a = 2^p - 1$, and assume a is prime. We want to look at $\left(\frac{3}{a}\right)$, we also know that $p > 2$ (if $p = 2$, then $a = 3$, but we are only worried about Mersenne primes greater than 3), which means that p must be odd. Let's think about what a is mod 4. Since $p > 2$, then $a \equiv 3 \pmod 4$, since

$2^p \equiv 0 \pmod 4$ when $p \geq 2$. So we can use quadratic reciprocity to do the following,

$$\begin{aligned}
\left(\frac{3}{a}\right) &= -\left(\frac{a}{3}\right) \\
&\equiv -\left(2^p - 1\right)^{\frac{3-1}{2}} \pmod 3 \\
&\equiv -\left(2^p - 1\right) \pmod 3
\end{aligned}$$

Because p is odd, we know $2^p \equiv 2 \pmod 3$

$$\begin{aligned}
&\equiv -(2-1) \pmod 3 \\
&\equiv -1 \pmod 3 \\
\left(\frac{3}{a}\right) &= -1
\end{aligned}$$

So we can see that 3 is a quadratic nonresidue for all Mersenne primes greater than 3.

Problem 4.

(a) Prove that if $p \equiv 7 \pmod 8$, then $p | \left(2^{\left(\frac{(p-1)}{2}\right)} - 1\right)$

(b) Find a factor of $2^{83} - 1$

Solution.

(a) *Proof.* Let $p \equiv 7 \pmod 8$. Then, based on theorem 2 in chapter 12, we know that $\left(\frac{2}{p}\right) = 1$, which is the same as saying $2^{\left(\frac{(p-1)}{2}\right)} - 1 \equiv 0 \pmod p$, which is then also the same as saying $p | \left(2^{\left(\frac{(p-1)}{2}\right)} - 1\right)$. $\square$

(b) If we look for a p where $\frac{p-1}{2} = 83$, we find $p = 167$, and since $167 \equiv 7 \pmod 8$, we can use the above to see that $167 | 2^{83}$.

Problem 5.

(a) If p and $q = 10p + 3$ are odd primes, show that $\left(\frac{p}{q}\right) = \left(\frac{3}{p}\right)$.

(b) If p and $q = 10p + 1$ are odd primes, show that $\left(\frac{p}{q}\right) = \left(\frac{-1}{p}\right)$

Solution.

(a) *Proof.* Let p and $q = 10p + 3$ be odd primes. If $p \equiv 3 \pmod 4$, then

$$\begin{aligned} q &\equiv 10(3) + 3 \pmod 4 \\ q &\equiv 33 \pmod 4 \\ q &\equiv 1 \pmod 4 \end{aligned}$$

So no matter what at least one of p or q will be not equivalent to 3 mod 4, so we know that we can apply quadratic reciprocity as follows,

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) \\ &= \left(\frac{10p+3}{p}\right) \\ \left(\frac{p}{q}\right) &= \left(\frac{3}{p}\right) \end{aligned}$$

$\square$

(b) *Proof.* Let p and $q = 10p + 1$ be odd primes. If $p \equiv 3 \pmod 4$, then

$$\begin{aligned} q &\equiv 10(3) + 1 \pmod 4 \\ q &\equiv 31 \pmod 4 \\ q &\equiv 3 \pmod 4 \end{aligned}$$

So when $p \equiv 3 \pmod 4$, we have

$$\begin{aligned} \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right) \\ &= -\left(\frac{10p+1}{p}\right) \\ \left(\frac{p}{q}\right) &= -\left(\frac{1}{p}\right) \\ \left(\frac{p}{q}\right) &= -1 \end{aligned}$$

If $p \equiv 1 \pmod 4$, we have

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) \\ &= \left(\frac{10p+1}{p}\right) \\ \left(\frac{p}{q}\right) &= \left(\frac{1}{p}\right) \\ \left(\frac{p}{q}\right) &= 1 \end{aligned}$$

Which we can see is the same definition as $\left(\frac{-1}{p}\right)$, so $\left(\frac{p}{q}\right) = \left(\frac{-1}{p}\right)$ $\square$

Problem 6.

(a) Which primes can divide $n^2 + 1$ for some n?

(b) Which odd primes can divide $n^2 + n$ for some n?

(c) Which odd primes can divide $n^2 + 2n + 2$ for some n?

Solution.

(a) Let p be some odd prime, we want to know for what p we have $p|n^2 + 1$ for some n. This can be rewritten as finding when

$$\begin{aligned} n^2 + 1 &\equiv 0 \pmod p \\ n^2 &\equiv -1 \pmod p \end{aligned}$$

This can be rewritten as when $\left(\frac{-1}{p}\right) = 1$. So an odd prime can divide $n^2 + 1$ for some n if and only if $p \equiv 1 \pmod 4$, and when $p = 2$, (since $1 \equiv -1 \pmod 2$, so $1^2 \equiv -1 \pmod 2$).

(b) We are looking for when $p|n^2 + n$ for some n, this can be rewritten as finding when

$$\begin{aligned} n^2 + n &\equiv 0 \pmod p \\ n^2 &\equiv -n \pmod p \end{aligned}$$

This can be rewritten as when $\left(\frac{-n}{p}\right) = 1$. So an odd prime can divide $n^2 + n$, for some n if and only if $\left(\frac{-n}{p}\right) = 1$.

(c) We are looking for when $p|(n^2 + n + 2)$ for some n, this can be rewritten as finding when

$$\begin{aligned} n^2 + n + 2 &\equiv 0 \pmod p \\ n^2 &\equiv -(n+2) \pmod p \end{aligned}$$

This can be rewritten as when $\left(\frac{-(n+2)}{p}\right) = 1$. So an odd prime can divide $n^2 + n + 2$, for some n if and only if $\left(\frac{-(n+2)}{p}\right) = 1$.

Problem 7.

(a) Show that if $p \equiv 3 \pmod 4$ and a is a quadratic residue $\pmod p$, then $p - a$ is a quadratic nonresidue $\pmod p$.

(b) What if $p \equiv 1 \pmod 4$?

Solution.

(a) Let $p \equiv 3 \pmod 4$, and let a be a quadratic residue $\pmod p$, then look at

$$\begin{aligned} \left(\frac{p-a}{p}\right) &= \left(\frac{-a}{p}\right) \\ &= \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) \\ &= \left(\frac{-1}{p}\right) \\ \left(\frac{p-a}{p}\right) &= -1 \end{aligned}$$

Which is the definition of $p - a$ being a quadratic nonresidue $\pmod p$.

(b) We can see that the argument doesn't change up until the last step when evaluating $\left(\frac{-1}{p}\right)$, so if $p \equiv 1 \pmod 4$, $p - a$ is a quadratic residue $\pmod p$.

3

Problem. If p is an odd prime, prove that

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$

Proof. Let p be an odd prime, then we know that for any a (where a is a proper residue mod p) has the same square outcome as $-a$, so at most we can have $\frac{p-1}{2}$ quadratic residues for p, however, we know that we can't have a, b, in mod p where $a \not\equiv \pm b \pmod p$ but $a^2 \equiv b^2 \pmod p$, so we will actually have exactly $\frac{p-1}{2}$ quadratic residues for p, meaning we will also have exactly $\frac{p-1}{2}$ quadratic nonresidues. This means that there is an equal number of them that will be 1 and -1, so it will sum to 0. ☐

4

Problem. For which primes $p = 3, 5, 7, 11, 13, 17$ does $x^2 \equiv -2 \pmod p$ have a solution? Which primes in general guarantee solutions to this equation? Can you prove it?

Proof. $x^2 \equiv -2 \pmod p$ will have solutions when either both $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$ are equal to 1 or equal to -1. We know that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

And that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

So we need $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 8$, which can be written as just $p \equiv 1 \pmod 8$ since if $p = 8k + 1$, this implies that $p \equiv 1 \pmod 4$ as well, the same argument is true for when $p \equiv 3 \pmod 8$. The other two cases do not work since they flip the polarity when in the other modulus, so -2 is a quadratic residue when $p \equiv 1 \pmod 8$ or when $p \equiv 3 \pmod 8$. So $x^2 \equiv -2 \pmod p$ has solutions for $p = 3, 11$, and 17. □

5

Problem. Let $p \equiv 1 \pmod 4$ and denote both solutions of $x^2 \equiv -1 \pmod p$ by i and $-i$. Prove or disprove:

$$\text{If } a + bi \equiv 0 \pmod p \text{ then } a \equiv b \equiv 0 \pmod p$$

Proof. Let $p \equiv 1 \pmod 4$ and let i and $-i$ be the two solutions of $x^2 \equiv -1 \pmod p$. Then let's look at

$$\begin{aligned} a + bi &\equiv 0 \pmod p \\ (a + bi)(a - bi) &\equiv 0 \pmod p \\ a^2 - b^2(-1) &\equiv 0 \pmod p \\ a^2 + b^2 &\equiv 0 \pmod p \end{aligned}$$

We know that this can be solved for $a \not\equiv b \not\equiv 0$ because $p \equiv 1 \pmod 4$, so there exists $c^2 \equiv -1$ and we can let a or b be -1 and the other the solution. So the statement is false. □

6

Problem. If $p \equiv 7 \pmod 8$ and $h = \frac{(p-1)}{2}$ is prime, evaluate $\left(\frac{h}{p}\right)$.

Proof. If $p \equiv 7 \pmod 8$, then we know that $\left(\frac{2}{p}\right) = 1$, so since $h \perp 2$ (since h is prime) we can see this means that $\left(\frac{h}{p}\right) = \left(\frac{2h}{p}\right)$, so we can do the following

$$\begin{aligned}
\left(\frac{h}{p}\right) &= \left(\frac{2h}{p}\right) \\
&= \left(\frac{p+1}{p}\right) \\
&= \left(\frac{1}{p}\right) \\
\left(\frac{h}{p}\right) &= 1
\end{aligned}$$

$\square$

7

Problem. For the following values of n and e, find the magic decoding exponent d **by hand**. You may use a calculator for large computations if needed but please show your steps.

(a) $n = 17$, $e = 5$

(b) $n = 21$, $e = 11$

Solution.

(a) We have $y \equiv x^5 \pmod{17}$, and we want to find d s.t. $y^d \equiv x \pmod{17}$. Our n is prime, so we want d s.t. $(n-1)t + 1 = ed$ for some t or $5d \equiv 1 \pmod{16}$. So let's create a chart for mod 16 as follows:

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$5a \pmod{16}$	0	5	10	15	4	9	14	3	8	13	2	7	12	1	6	11

So we can see that $d = 13$. We can check this by seeing that

$$\begin{aligned}
(x^5)^{13} &\equiv x^{65} && \pmod{17} \\
&\equiv x^{65} && \pmod{17} \\
&\equiv (x^{16})^4 \cdot x && \pmod{17} \\
&\equiv 1^4 \cdot x && \pmod{17} \\
(x^5)^{13} &\equiv x \quad \checkmark && \pmod{17}
\end{aligned}$$

(b) We have $y \equiv x^{11} \pmod{21}$, and we want to find d s.t. $y^d \equiv x \pmod{21}$. Our n here is $3 \cdot 7$, so here we want to find $\phi(n)t + 1 = ed$ for some t, or $11d \equiv 1 \pmod{\phi(21)}$. First we need to find $\phi(21)$, which we can find by doing

$$\begin{aligned}\phi(21) &= 21\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)\\ &= 21\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\\ \phi(21) &= 12\end{aligned}$$

So let's create a chart for mod 12 as follows using that $11 \equiv -1 \pmod{12}$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$-a \pmod{12}$	0	11	10	9	8	7	6	5	4	3	2	1

So we can see that $d = 11$. We can check this by seeing that

$$\begin{aligned}(x^{11})^{11} &\equiv x^{121} && \pmod{21}\\ &\equiv (x^{12})^{10}\cdot x && \pmod{21}\\ &\equiv (1)^{10}\cdot x && \pmod{21}\\ (x^{11})^{11} &\equiv x \quad \checkmark && \pmod{21}\end{aligned}$$

8

Problem. Find the rational number, in lowest, terms, given by each of the following continued fractions

(a) [3,2,1]

(b) [3,7,15,1]

Solution.

(a)

$$\begin{aligned}[3,2,1] &= 3+\frac{1}{2+\frac{1}{1}}\\ &= 3+\frac{1}{3}\\ &= \frac{10}{3}\end{aligned}$$

(b)

$$
\begin{aligned}
[3,7,15,1] &= 3+\cfrac{1}{7+\frac{1}{15+\frac{1}{1}}}\\
&= 3+\cfrac{1}{7+\frac{1}{16}}\\
&= 3+\cfrac{1}{\frac{113}{16}}\\
&= 3+\frac{16}{113}\\
[3,7,15,1] &= \frac{355}{113}
\end{aligned}
$$

9

Problem. Find the simple continued fraction expansion for the following values:

(a) $\frac{32}{17}$

(b) $\sqrt{3}$

Solution.

(a)

$$
\begin{aligned}
\frac{32}{17} &= 1+\frac{15}{17}\\
&= 1+\cfrac{1}{\frac{17}{15}}\\
&= 1+\cfrac{1}{1+\frac{2}{15}}\\
&= 1+\cfrac{1}{1+\frac{1}{\frac{15}{2}}}\\
&= 1+\cfrac{1}{1+\frac{1}{7+\frac{1}{2}}}\\
\frac{32}{17} &= [1,1,7,2]
\end{aligned}
$$

(b) We can start with $\alpha = \sqrt{3} = \alpha_1$, then $a_1 = \lfloor\sqrt{3}\rfloor = 1$

Then, $\alpha_2 = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$, and $a_2 = \lfloor\frac{\sqrt{3}+1}{2}\rfloor = 1$.

Then, $\alpha_3 = \frac{1}{\frac{\sqrt{3}+1}{2}-1} = \frac{1}{\frac{\sqrt{3}+1-2}{2}} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{2} = \sqrt{3}+1$ and $a_3 = \lfloor\sqrt{3}+1\rfloor = 2$.

Then, $\alpha_4 = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \alpha_2$, so $a_4 = a_2$.

So $\sqrt{3} = [1, \overline{1, 2}]$

10

Problem. Find the exact value of he following continued fractions

(a) $[1, \overline{2}] = [1, 2, 2, 2, 2, \cdots]$

(b) $[3, \overline{2, 6}] = [3, 2, 6, 2, 6, 2, 6, \cdots]$

Solution.

(a) We can use the theorem of $[a, \overline{b}] = \frac{2a-b}{2} + \frac{\sqrt{b^2+4}}{2}$ to see that

$$\begin{aligned} [1, \overline{2}] &= \frac{2(1)-2}{2} + \frac{\sqrt{2^2+4}}{2} \\ &= \frac{\sqrt{8}}{2} \\ &= \frac{2\sqrt{2}}{2} \\ [1, \overline{2}] &= \sqrt{2} \end{aligned}$$

(b) We can start by finding $[\overline{2, 6}]$ by letting $a = [\overline{2, 6}]$ and letting

$$\begin{aligned} a &= 2 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{\ddots}}}} \\ a &= 2 + \frac{1}{6 + \frac{1}{a}} \\ a &= 2 + \frac{1}{\frac{6a+1}{a}} \\ a &= 2 + \frac{a}{6a+1} \\ a &= \frac{2(6a+1)+a}{6a+1} \\ a &= \frac{13a+2}{6a+1} \\ 6a^2 + a &= 13a + 2 \\ 0 &= 6a^2 - 12a - 2 \end{aligned}$$

Then we can use the quadratic formula to get

$$\begin{aligned}
a &= \frac{12 \pm \sqrt{(-12)^2 - 4(6)(-2)}}{2(6)} \\
a &= \frac{12 \pm \sqrt{144 + 48}}{12} \\
a &= \frac{12 \pm \sqrt{192}}{12} \\
a &= \frac{12 \pm 8\sqrt{3}}{12} \\
a &= \frac{3 \pm 2\sqrt{3}}{3}
\end{aligned}$$

We only care about the positive case here. Then, we can see that

$$\begin{aligned}
[3, \overline{2, 6}] &= 3 + \frac{1}{a} \\
&= 3 + \frac{1}{\frac{3+2\sqrt{3}}{3}} \\
&= 3 + \frac{3}{3 + 2\sqrt{3}} \\
&= \frac{3(3 + 2\sqrt{3}) + 3}{3 + 2\sqrt{3}} \\
&= \frac{12 + 6\sqrt{3}}{3 + 2\sqrt{3}} \\
&= \frac{12 + 6\sqrt{3}}{3 + 2\sqrt{3}} \cdot \frac{3 - 2\sqrt{3}}{3 - 2\sqrt{3}} \\
&= \frac{(12 + 6\sqrt{3})(3 - 2\sqrt{3})}{9 - 12} \\
&= \frac{36 - 24\sqrt{3} + 18\sqrt{3} - 36}{-3} \\
&= \frac{-6\sqrt{3}}{-3} \\
[3, \overline{2, 6}] &= 2\sqrt{3}
\end{aligned}$$