Math 110AH Homework 2

Nathan Solomon

October 19, 2023

Assignment due October 18th at 11:59 pm

Note to grader: please look at all the questions and let me know how this would be scored if it were an exam.

1. Prove that if $a \equiv b \pmod{m}$, then $\gcd(m, a) = \gcd(m, b)$.

Let $d = \gcd(m, a)$. Then d divides m, and since $a - b$ is an integer multiple of m, d must divide $a - b$ as well. Also, d divides a, which means d divides $a + (a - b)$. Since d divides both b and m, we know that $\gcd(m, b)$ has to be at least d. That is,

$$\gcd(m, a) \leq \gcd(m, b).$$

Repeating that logic but with a and b swapped, we see that

$$\gcd(m, b) \leq \gcd(m, a),$$

which implies both sides are equal.

2. Prove that $(a + b)^p \equiv a^p + b^p \pmod{p}$ if p is prime.

Proof outline: expand the left-hand-side using the binomial theorem, then prove that the coefficient of every term other than a^p and b^p is divisible by p.

Consider the n^{th} term in that expansion (assume n starts counting at zero):

$$\binom{p}{n} \cdot a^{p-n}b^n := \frac{p!}{n!(p-n)!} \cdot a^{p-n}b^n$$

The numerator of the fraction on the right-hand-side is divisible by p, but when $1 \leq n \leq p-1$, $n!$ and $(p - n)!$ are not divisible by p. Since p is prime, that implies the denominator is not divisible by p. Using induction with Pascal's identity, one could easily prove that binomial coefficients are always integers, meaning the numerator is an integer multiple of the denominator.

Since the numerator is divisible by p and the denominator isn't, that quotient must be an integer multiple of p. Therefore the coefficient of the n^{th} term is an integer multiple of

p, and since $a^{p-n}b^n$ is also an integer, the n^{th} term of the binomial expansion is an integer multiple of p whenever $1 \leq n \leq p-1$.

Now we can rewrite the left hand side of the given equation by ignoring all integer multiples of p:

$$\begin{aligned}(a+b)^p &= \sum_{n=0}^{p} \binom{n}{p} a^{p-n}b^n \\ &= \binom{p}{0}a^pb^0 + \binom{p}{1}a^{p-1}b^1 + \cdots + \binom{p}{p}a^0b^p \\ &\equiv \binom{p}{0}a^pb^0 + [0+0+\cdots+0] + \binom{p}{p}a^0b^p \pmod{p} \\ &\equiv a^p + b^p \pmod{p}.\end{aligned}$$

3. Find all classes $X \in \mathbb{Z}/300\mathbb{Z}$ such that:

- (i) $[7] \cdot X = [2]$,
- (ii) $[120] \cdot X = [80]$,
- (iii) $[9] \cdot X = [48]$.

```
>>> def get_answer(a, b):
...     return [x for x in range(300) if a*x % 300 == b]
...
>>> get_answer(7, 2)
[86]
>>> get_answer(120, 80)
[]
>>> get_answer(9, 48)
[72, 172, 272]
```

- (i) Proof by exhaustion: $X = \{[86]\}$.
- (ii) There are no solutions, because $[120] \cdot X$ must be a multiple of $[3]$, but $[80]$ is not a multiple of $[3]$. In other words, $\{[0], [3], [6], \ldots, [297]\}$ is a subgroup of $\mathbb{Z}/300\mathbb{Z}$. If that's not rigorous enough, I also did a proof by exhaustion.
- (iii) Proof by exhaustion: $X = \{[72], [172], [272]\}$.

4. Find all positive $m \in \mathbb{Z}$ such that $[5] \cdot [17] = [3] \cdot [4]$ in $\mathbb{Z}/m\mathbb{Z}$.

First, note that $[5]\cdot[17] = [3]\cdot[4]$ if and only if $[85] = [12]$, which is equivalent to $[73] = [0]$. This is possible if and only if m divides 73, but since 73 is prime, the only solutions are $m = 1$ and $m = 73$.

5. Prove that every nonzero class $[a] \in \mathbb{Z}/13\mathbb{Z}$ is equal to $[2]^i$ for some i.

```
>>> print([2**i % 13 for i in range(13)])
[1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1]
```

The numbers listed above are the consecutive powers of [2]. Since there are 12 unique nonzero numbers there (which are precisely the nonzero classes $[a] \in \mathbb{Z}/13\mathbb{Z}$), every nonzero class $[a]$ is equal to $[2]^i$ for some i.

6. Find the (multiplicative) inverse of [100] in $\mathbb{Z}/173\mathbb{Z}$.

```
>>> for i in range(173):
...     if i * 100 % 173 == 1:
...             print(i)
...
109
>>> 10900%173
1
>>> (100*109-1)/173
63.0
```

$100 \cdot 109 = 1 + 173 \cdot 63$ which means $[100]^{-1} = [109]$. Since 173 is prime, that multiplicative inverse is unique (although we also saw from the python code above that $x = [109]$ is the only solution to $[100] \cdot x = [1]$).

7. Solve $X^2 = [5]$ in $\mathbb{Z}/11\mathbb{Z}$.

```
>>> for x in range(11):
...     if x**2 % 11 == 5:
...             print(x)
...
4
7
```

So by exhaustion, the only solutions are $X = [4]$ and $X = [7]$.

8. Find all $k \in \mathbb{N}$ such that $[2]^k = [1]$ in $\mathbb{Z}/17\mathbb{Z}$.

The following code snippit shows that the smallest positive integer k satisfying $[2]^k = [1]$ is 8:

```
>>> k = 1
>>> while 2**k % 17 != 1:
...     k += 1
...
>>> print(k)
8
>>> 2**8 % 17
1
```

According to the division theorem, for any integer k, there exist integers q and r such that $k = 8q + r$ and $0 \leq r < 8$ (and since k is positive, we also know that q is non-negative). Then $[2]^k = [2]^{8q} \cdot [2]^r = [1]^q \cdot [2]^r = [2]^r$. But we already checked all 8 possible values of $[2]^r$, and the only one which satisfies $[2]^r = [1]$ is $r = 0$. Therefore the equation is true if and only if $k \in 8\mathbb{N}$.

That's not quite true – k can actually be any integer multiple of 8, but the question only asked for the nonnegative solutions.

9. Let X be the set of all pairs $(a, b), a, b \in \mathbb{R}$ such that $a^2 + b^2 > 0$. We write $(a, b) \sim (c, d)$ if $ad = bc$. Show that $\sim$ is an equivalence relation and determine all equivalence classes.

Reflexivity. $(a, b) \sim (a, b)$ because $ab = ba$.

Symmetry. If $(a, b) \sim (c, d)$ then $(c, d) \sim (a, b)$ because $ad = bc$ implies $cb = ad$. If $(a, b) \not\sim (c, d)$ then $(c, d) \not\sim (a, b)$ because $ad \neq bc$ implies $cb \neq ad$.

Transitivity. If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ then $(a, b) \sim (e, f)$. This works because if $ad = bc$ and $cf = de$, then $c = de/f$, so $ad = b(de/f)$, so $af = be$.

The equivalence class of (a, b) is the set of points $(x, y) \in \mathbb{R}^2$ such that $y = bx/a$ (unless $a = 0$), which is the line through the origin with slope b/a (or a vertical line when $a = 0$). Therefore the set of all equivalence classes is the set of lines in $\mathbb{R}^2$ that pass through the origin.

10. Prove that $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ for every odd integer a and every $n \geq 3$.

Since a is odd, it can be written as $a = 2k + 1$ for some integer k.

In the base case, $n = 3$. The statement is true in that case because

$$\begin{aligned} a^{2^{n-2}} &= a^2 \\ &= 1 + (a + 1) \cdot (a - 1) \\ &= 1 + (2k + 2) \cdot (2k) \\ &= 1 + 4k^2 + 4k \\ &\equiv 1 \pmod{2^n}. \end{aligned}$$

That last step works because either k or $k + 1$ has to be even, so their product is even, and we can conclude $4k^2 + 4k$ is a multiple of 8.

Now for the inductive step, we suppose the statement is true when $n = n_0$, and use that to show that it is also true when $n = n_0 + 1$. Consider the quantity

$$x := a^{2^{n_0-2}}.$$

Since we assumed the statement is true when $n = n_0$, we know that x is congruent to 1 (modulo 2^{n_0}) – that is, there exists an integer c such that $x = 1 + 2^{n_0}c$. That means

$$\begin{aligned} x^2 &= (2^{n_0})^2c^2 + 2 \cdot 2^{n_0}c + 1 \\ &= 1 + 2^{n_0+1}(c + 2^{n_0-1}) \end{aligned}$$

which implies

$$a^{2^{(n_0+1)-2}} = x^2 \equiv 1 \pmod{2^{n_0+1}}.$$

We have proven that the statement

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

is true when $n = 3$, and that if it's true when $n = n_0$, it must also be true when $n = n_0 + 1$. So by induction, it's true for any integer $n \geq 3$.