Number Theory Homework IV

RDB

June 26, 2022

In general, assume that variables like n, m, and k are integers.

Exercise 1 Prove that, if integers a and b divide an integer c, and $\gcd(a, b) = 1$, then ab divides c.

Solution 1

I think we already did this one. Didn't we do Bézout's lemma? Let's do it another way.

The prime factorization of c contains primes from a and b, but there is no overlap between them since $\gcd(a, b) = 1$. The product ab just mashes those distinct primes together, so ab divides c.

To be a little more formal, write $a = p_1^{e_1} \cdots p_m^{e_m}$ and $b = q_1^{r_1} \cdots q_k^{r_k}$, where the p_i's and q_k's are distinct primes. Since a and c both divide c, these prime factorizations must appear in the factorization of c as well:

$$\begin{aligned} c &= (p_1^{e_1} \cdots p_m^{e_m})(q_1^{r_1} \cdots q_k^{r_k})x \\ &= abx, \end{aligned}$$

where x is some integer.

Exercise 2 Find the general solution to the following congruence systems.

(**a**)

$$\begin{aligned} 2x &= 0 \pmod 5 \\ x &= -1 \pmod 3 \end{aligned}$$

(**b**)

$$\begin{aligned} x &= 1 \pmod 3 \\ x &= 2 \pmod 5 \\ x &= 3 \pmod 7 \end{aligned}$$

Solution 2

(**a**) (5 points) The CRT tells us that this has a single solution mod 15. This gives us a few ways to find it.

i. Ad-hoc thinking: $5 \mid 2x$ iff $5 \mid x$, so we are looking for a multiple of 5 that is congruent to -1 (or 2) mod 3. The multiples of 5 are 0, 5, and 10. It's clear that $x = 5$ will work, so that's the particular solution.

ii. Use the CRT formula. Particular solutions are $x_1 = 0$ and $x_2 = -1$. Thus, we can take

$$\begin{aligned} x_0 &= x_1 3(3)^{-1} + x_2 5(5)^{-1} \\ &= (-1)5 \cdot 2 \\ &= -10. \end{aligned}$$

(The inverse of 5 mod 3 is 2, since $5 \cdot 2 = 10 \equiv 1 \pmod 3$.)

iii. Just guess. There are only 15 values to check, so keep going until you hit $x = 5$.

Once you have a particular solution x_0, every other solution is of the form

$$x = x_0 + 15k$$

for some integer k.

(**b**) (5 points) Same idea before, except now with three equations. Don't forget to read the book! You can do the same ad-hoc idea (see Problem 3 below for an example), or you can use the formula. Here's what the formula looks like.

Particular solutions are $x_1 = 1$, $x_2 = 2$, and $x_3 = 3$. The formula is

$$x_0 = x_1(m_2m_3)(m_2m_3)^{-1} + x_2(m_1m_3)(m_1m_3)^{-1} + x_3(m_1m_2)(m_1m_2)^{-1}.$$

In this case, $m_2m_3 = 35 \equiv 2 \pmod 3$, so $(m_2m_3)^{-1} = 2$. Similarly, $m_1m_3 = 21 \equiv 1 \pmod 5$, so $(m_1m_3)^{-1} = 1$, and $m_1m_2 = 15 \equiv 1 \pmod 7$, so $(m_1m_2)^{-1} = 1$. Plugging all this in, we get

$$\begin{aligned} x_0 &= 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \\ &= 70 + 42 + 45 \\ &= 157. \end{aligned}$$

So the general solution is

$$x = 157 + 3 \cdot 5 \cdot 7k = 157 + 105k.$$

(By shifting back, you can see that the smallest solution is 52.)

Exercise 3

(**a**) Show that if $m_1, m_2, \ldots, m_n$ is any sequence of positive integers which are pairwise relatively prime, then there exist n consecutive positive integers x, $x+1$, $\ldots$, $x+n-1$ such that x is divisible by m_1, $x+1$ is divisible by m_2, and so on. [Hint: Chinese Remainder Theorem.]

(**b**) Let the primes be enumerated by $\{p_n\}_{n\geq 1}$. That is, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so on.

Prove that, for any n, there exist n consecutive positive integers x, $x+1$, $\ldots$, $x+n-1$ such that the first is divisible by p_1, the second by p_2, the third by p_3, and so on. What is the *smallest* positive x when $n = 3$?

Solution 3

(**a**) (5 points) This is equivalent to

$$\begin{aligned} x &\equiv 0 \pmod{m_1} \\ x &\equiv -1 \pmod{m_2} \\ &\vdots \\ x &\equiv -(n-1) \pmod{m_n}. \end{aligned}$$

By the CRT, this has a particular solution x_0, and all other solutions are of the form

$$x = x_0 + m_1 m_2 \cdots m_n t$$

for some integer t. In particular, we can get $x > 0$ by choosing a sufficiently large t.

(**b**) (5 points) The existence of a solution is just the previous part with $m_k = p_k$. For $n = 3$, the equations are

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv -1 \pmod{3} \\ x &\equiv -2 \pmod{5}. \end{aligned}$$

The CRT says that there is a unique solution mod $2 \cdot 3 \cdot 5 = 30$. That's a few too many to check all of them, but we can start by looking at multiples of 5 minus 2:

$$-2, 3, 8, 13, 18, 23, 28.$$

Which of these are even?

$$-2, 8, 18, 28.$$

Which of these are congruent to -1 mod 3?

$$8.$$

So $x = 8$ is the smallest positive integer such that $2 \mid x$, $3 \mid x + 1$, and $5 \mid x + 2$.

Exercise 4 A class in number theory was to divide itself into groups of equal sizes to study the Chinese Remainder Theorem. When the class was divided into groups of 3, two students were left out; when into groups of 4, one was left out. When it was divided into groups of five, the students found that if the professor was added to one of the groups, no one was left out. Since the professor had never really understood the Chinese Remainder Theorem when he was in college, the last arrangement worked out nicely. How many students were there in the class? [Assume that the class is as small as possible.]

Solution 4
(10 points)

Let x be the size of the class. When the class was divided into groups of three, two students were left out. Therefore $x \equiv 2 \pmod 3$. When the class was divided into groups of four, one student was left out. Therefore $x \equiv 1 \pmod 4$. When the class was divided into groups of five, they were one short of being perfect. Therefore $x + 1 \equiv 0 \pmod 5$. All together, we have the following equations:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv -1 \pmod 5. \end{aligned}$$

The Chinese Remainder Theorem tells us that there is a unique solution mod $3 \cdot 4 \cdot 5 = 60$.

At this point, you could go look up the three-equation formula to get a particular solution in the book. The particular solutions are easy: $x_1 = 2$, $x_2 = 1$, and $x_3 = -1$. However, this is a little annoying. Another way is to look at the multiples of five minus one:

$$-1, 4, 9, 14, 19, 24, 29, 34, 39, 44, 49, 54, 59.$$

These satisfy the first equation. Now only take the ones that are congruent to 1 mod 4:

$$9, 29, 49.$$

Now take the ones that are congruent to 2 mod 3:

$$29.$$

The unique solution mod 60 is $x = 29$.

Exercise 5 Find three consecutive positive integers such that the first is divisible by the square of a prime, the second by the cube of a prime, and the third by the fourth power of a prime. [The prime does not have to be the same for each integer.]

Solution 5
Consider the following congruence:

$$\begin{aligned} x &\equiv 0 \pmod{2^2} \\ x+1 &\equiv 0 \pmod{3^3} \\ x+2 &\equiv 0 \pmod{5^4}. \end{aligned}$$

It does not seem obvious that this should be true at all, but the Chinese Remainder Theorem tells us that it *does* happen. In fact, it only happens once mod 67500!

The problem at this point is that this is a really big range. To solve this one with paper and pencil, you would really need to to use the general formula from Chapter 5. However, the vastly superior way to do it is to write a small little program:

```
[k for k in range(67500)
    if            k % 2**2 == 0
        and (k + 1) % 3**3 == 0
        and (k + 2) % 5**4 == 0]
```

It spits out `[21248]`, and it's not hard to check that that works.

Exercise 6 Fix relatively prime integers a and b. Use the Chinese Remainder theorem to show that every common multiple of a and b is divisible by ab.

Solution 6
(5 points) An integer x is a common multiple of a and b iff

$$\begin{aligned} x &= 0 \pmod{a} \\ x &= 0 \pmod{b}. \end{aligned}$$

By the Chinese Remainder Theorem, this has a unique solution mod ab. Since $x = 0$ is a solution, it follows that every common multiple of a and b is congruent to 0 mod ab.

Exercise 7 If $x^2 \equiv a \pmod{m}$, then we say that x is a *square root* of a mod m.

(**a**) (2 points) Prove that the square roots of 1 mod p are ± 1 when p is prime. That is, show that the equation $x^2 = 1 \pmod{p}$ has exactly two incongruent solutions, 1 and -1.

(**b**) (2 points) Prove that $a \neq 0$ has either zero or two square roots mod p if $p \geq 3$ is prime. Prove that $a = 0$ has exactly one square root mod p.

(**c**) (1 point) Show that 0 has more than two square roots mod 36.

Solution 7

(**a**) The equation is equivalent to $p \mid (x^2 - 1)$, or $p \mid (x-1)(x+1)$. Since p is prime, it must divide one of the two factors. That is, either $p \mid (x-1)$ or $p \mid (x+1)$. This is another way to say that $x \equiv \pm 1 \pmod{p}$.

(**b**) If $x^2 \equiv a \pmod{p}$, then $(-x)^2 = x^2 \equiv a \pmod{p}$, so x and $-x$ are *both* square roots of a. The problem is that sometimes $x \equiv -x \pmod{p}$. This means that $p \mid 2x$, so either $p \mid 2$ or $p \mid x$. The former implies $p = 2$, and the latter implies $a \equiv 0 \pmod{p}$.

On the other hand, if $a \equiv 0 \pmod{p}$, then $x^2 \equiv 0 \pmod{p}$ implies $p \mid x^2$, so $p \mid x$. Thus every square root of 0 is 0 mod p.

(**c**) Both 0^2 and 6^2 are congruent to 0 mod 36, yet they are not congruent to each other mod 36.

Exercise 8 This exercise involves programming.

Say that a positive integer $n > k > 0$ is *k-divisible* if n is divisible by $n - k$.

(**a**) Prove that $k \leq n \leq 2k$ if n is k-divisible. [Hint: The smallest multiple of $n - k$ is $2(n-k)$.]

(**b**) Write a function `findDivisibles(k)` which takes an integer k and returns all n which are k-divisible. [Hint: You only need to look at $k \leq n \leq 2k$ by the previous part.]

(**c**) For $1 \leq k \leq 20$, compute D_k, the number of k-divisible integers n. Look the values of D_k up in the OEIS. What entry seems most likely? Does the OEIS contain this conjecture?

Solution 8

(**a**) Since n is a multiple of $n-k$, but not equal to $n-k$ (since $k > 0$, we must have $n \geq 2(n-k)$. Writing this gives $n \leq 2k$.

(**b**)
```
def findDivisibles(k):
    return [n for n in range(k + 1, 2 * k + 1)
                if n % (n - k) == 0]
```

(**c**) Using the code `[len(findDivisibles(k) for k in range(1, 21)]`, I get the following values:

$$1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, 4, 5, 2, 6, 2, 6.$$

It looks like—maybe!—this is equal to the number of divisors of k, which is A000005 in the OEIS.

You don't have to know this next part. It's just some fun thing I found while writing the homework.

Proposition *The number of k-divisible integers equals $d(k)$, the number of divisors of k.*

Proof If n is k-divisible, then $n = (n-k)d$ for some unique integer d. Rewriting this, we have

$$dk = (d-1)n.$$

Since $\gcd(d-1, d) = 1$, it follows that $d-1$ divides k. That is, for every k-divisible integer d, we get a new divisor of k.

On the other hand, if l divides k, then let

$$n' = (l+1)(k/l),$$

which defines exactly one integer n'. Note that $ln' = (l+1)k$, so $(l+1)(n'-k) = n$, which shows that n is k-divisible. Thus, for every divisor of k, we get a new k-divisible integer.

Putting these two together, it follows that the number of k-divisible numbers is *exactly* $d(k)$. ■