CS 70 Fall 2021 — Discrete Mathematics and Probability Theory — HW 4

1 Modular Practice

Solve the following modular arithmetic equations for x and y.

(a) $9x+5 \equiv 7 \pmod{11}$.

(b) Show that $3x+15 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $3x+2y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2019} \equiv x \pmod{12}$.

(e) $7^{21} \equiv x \pmod{11}$.

(f) $x \equiv 5 \pmod{7}$, $x \equiv 3 \pmod{9}$, $x \equiv 3 \pmod{11}$. What is the smallest possible value for x?

Solution:

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{11}.$$

Now since $\gcd(9,11) = 1$, 9 has a (unique) inverse mod 11, and since $9 \times 5 = 45 \equiv 1 \pmod{11}$ the inverse is 5. So multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get:

$$x \equiv 10 \pmod{11}.$$

(b) Notice that any number $y \equiv 4 \pmod{21}$ can be written as $y = 4+21k$ (for some integer k). Evaluating y mod 3, we get $y \equiv 1 \pmod{3}$.

Since the right side of the equation is $1 \pmod{3}$, the left side must be as well. However, $3x+15$ will never be $1 \pmod{3}$ for any value of x. Thus, there is no possible solution.

(c) First, subtract the first equation from double the second equation to get:

$$2(2x+y)-(3x+2y) \equiv x \equiv 1 \pmod{7}.$$

Now plug into the second equation.

$$2+y \equiv 4 \pmod{7},$$

so the system has the solution $x \equiv 1 \pmod{7}$, $y \equiv 2 \pmod{7}$.

(d) We use the fact that

$$13 \equiv 1 \pmod{12}$$

Thus, we can rewrite the equation as $x \equiv 13^{2019} \equiv 1^{2019} \equiv 1 \pmod{11}$.

(e) One way to solve exponentiation problems is to test values until one identifies a pattern.

$$7^1 \equiv 7 \pmod{11}$$
$$7^2 \equiv 49 \equiv 5 \pmod{11}$$
$$7^3 = 7 * 7^2 \equiv 7 * 5 \equiv 2 \pmod{11}$$
$$7^4 = 7 * 7^3 \equiv 7 * 2 \equiv 3 \pmod{11}$$
$$7^5 = 7 * 7^4 \equiv 7 * 3 \equiv 10 \equiv -1 \pmod{11}$$

We theoretically could continue this until we the sequence starts repeating. However, notice that if $7^5 \equiv -1 \implies 7^{10} = (7^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}$.

Similarly, $7^{20} = (7^{10})^2 \equiv 1^2 \equiv 1 \pmod{11}$. As a final step, we have $7^{21} = 7 * 7^{20} \equiv 7 * 1 = 7 \pmod{11}$.

(f) Since the mod bases $7, 9, 11$ are all pairwise relatively prime, we can utilize the Chinese Remainder Theorem, which tells us there is a unique number $k \pmod{7 * 9 * 11}$ satisfying $k \equiv 5 \pmod{7}, k \equiv 3 \pmod{9}, k \equiv 3 \pmod{11}$.

Let's first try to satisfy the first two conditions. We're looking for a number k such that $k \equiv 5 \pmod{7}$ and $k \equiv 3 \pmod{9}$. Listing out the numbers $5 \pmod{7}$, we get:

$$5, 12, 19, 26, 33, 40, \ldots$$

By inspection, $k \equiv 12 \pmod{7 * 9}$ meets both requirements. Now we need to repeat the process to satisfy $k \equiv 3 \pmod{11}$ as well.

List out the numbers $k \equiv 12 \pmod{63}$ until we find one that meets the new condition as well. Doing so, we have:

$$12, 75, 138, 201, 264, \ldots$$

These numbers mod 11 are $1, 9, 6, 3, 0, \ldots$. Notice that adding 63 is the same as adding 8 in mod 11.

Here we select 201, which is the smallest number meeting all 3 conditions. Notice that all numbers $201 \pmod{693}$ work, but this question specifically asks for the smallest.

This trial-and-error strategy works well when the mods are small, but do note that there are many different ways to approach CRT problems.

2 Check Digits: ISBN

In this problem, we'll look at a real-world applications of check-digits.

International Standard Book Numbers (ISBNs) are 10-digit codes ($d_1 d_2 \ldots d_{10}$) which are assigned by the publisher. These 10 digits contain information about the language, the publisher, and the number assigned to the book by the publisher. Additionally, the last digit d_{10} is a "check digit" selected so that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \pmod{11}$. (*Note that the letter X is used to represent the number 10 in the check digit.*)

(a) Suppose you have a very worn copy of the (recommended) textbook for this class. You want to list it for sale online but you can only read the first nine digits: 0-07-288008-? (the dashes are only there for readability). What is the last digit? Show your work.

(b) Wikipedia says that you can determine the check digit by computing $\sum_{i=1}^{9} i \cdot d_i \pmod{11}$. Show that Wikipedia's description is equivalent to the above description.

(c) Prove that changing any single digit of the ISBN will render the ISBN invalid. That is, the check digit allows you to *detect* a single-digit substitution error.

(d) Can we ever switch two distinct digits in an ISBN number and get another valid ISBN number? For example, could 01$\underline{2}$34$\underline{5}$678X and 01$\underline{5}$34$\underline{2}$678X both be valid ISBNs? Explain.

Solution:

(a) $1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 + 10 \cdot d_{10} = 189 + 10 d_{10} \equiv 2 + 10 d_{10} \pmod{11}$. From the definition of the check digit, we know that $2 + 10 d_{10} \equiv 0 \pmod{11}$ so $10 d_{10} \equiv 9 \pmod{11}$. From here, we can quickly see that $d_{10} = 2$.

(b) It is sufficient to show that $d_{10} \equiv \sum_{i=1}^{9} i \cdot d_i \pmod{11}$ is a valid check digit (that is, that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \pmod{11}$). To see this, we note that

$$\begin{aligned}
\sum_{i=1}^{10} i \cdot d_i &= \sum_{i=1}^{9} i \cdot d_i + 10 \cdot d_{10} \\
&= \sum_{i=1}^{9} i \cdot d_i + 10 \cdot \sum_{i=1}^{9} i \cdot d_i \\
&= (1+10) \cdot \sum_{i=1}^{9} i \cdot d_i \\
&\equiv 0 \pmod{11}.
\end{aligned}$$

(c) Suppose that the correct digits are d_i (for $1 \le i \le 10$) and that the new digits are f_i. Since the question asks about a single substitution error, we will assume without loss of generality that the kth digit has been changed, i.e. $f_k \neq d_k$.

We proceed by proof by contradiction. Assume that the new ISBN is the same as previous one. Hence, we can write:

$$\sum_{i=1}^{10} i \cdot d_i \equiv \sum_{i=1}^{10} i \cdot f_i \pmod{11}.$$

Since only for the kth digit $f_k \neq d_k$, then

$$k \cdot d_k \equiv k \cdot f_k \pmod{11}.$$

Since 11 is prime and $1 \leq k \leq 10$, k has a (unique) inverse mod 11. We multiply the above equation by $k^{-1} \pmod{10}$.

$$d_k \equiv f_k \pmod{11}.$$

Since $1 \leq d_k \leq 10$ and $1 \leq f_k \leq 10$, then

$$d_k = f_k.$$

This is a contradiction, since at the beginning we assumed $f_k \neq d_k$. Hence, the the new ISBN is not the same as previous one and the error will be detected.

(d) Let's suppose that digits k and m are switched and all of the rest are left unchanged. We will write

$$f_i = \begin{cases} d_k, & i = m \\ d_m, & i = k \\ d_i, & \text{otherwise} \end{cases}$$

where $d_k \neq d_m$ (if they are equal, it's as if you never switched them so of course it will still be valid). Then we can write:

$$\begin{aligned}
\sum_{i=1}^{10} i \cdot f_i &= k \cdot d_m + m \cdot d_k + \sum_{i \neq k,m} i \cdot d_i \\
&= (k-m+m)d_m + (m-k+k)d_k + \sum_{i \neq k,m} i \cdot d_i && \text{note that } k-m+m = k \\
&= (k-m) \cdot d_m + (m-k) \cdot d_k + \sum_{i=1}^{10} i \cdot d_i && \text{bring like terms into the summation} \\
&= (k-m) \cdot d_m - (k-m) \cdot d_k + \sum_{i=1}^{10} i \cdot d_i \\
&= (k-m) \cdot (d_m - d_k) + \sum_{i=1}^{10} i \cdot d_i && \text{combine like terms} \\
&\equiv (k-m) \cdot (d_m - d_k) \pmod{11} && \text{by the definition of the check digit}
\end{aligned}$$

Since we know that $-9 \leq k - m \leq 9$, $k - m \neq 0$, $d_m - d_k \neq 0$, and 11 is prime, we know that this will not be equivalent to 0 mod 11, thus an error will be detected.

3 Divisible or Not

(a) Prove that for any number n, the number formed by the last two digits of n are divisible by 4 if and only if n is divisible by 4. (For example, ‘23xx’ is divisible by 4 if and only if the number ‘xx’ is divisible by 4.)

(b) Prove that for any number n, the sum of the digits of n are divisible by 3 if and only if n is divisible by 3.

Solution:

(a) Using modular arithmetic, we can prove both directions of the implication at once. Take n, which has k digits.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1} = \sum_{i=0}^{k-1} 10^i n_i$$

We can take $n \pmod 4$ and see that all terms n_2 up to n_{k-1} drop out since $10^2, 10^3, \ldots, 10^{k-1}$ are all divisible by 4.

$$n \equiv n_0 + 10n_1 \pmod 4$$

$n_0 + 10n_1$ is 0 in mod 4 if and only if n is 0 in mod 4, proving that the number formed by the last digits is divisible by 4 if and only if the entire number n is divisible by 4.

Let us now consider the alternative solution, where we do not use modular arithmetic.

Alternative Solution

Let P be "the last two digits of n are divisible by 4", and Q be "n is divisible by 4".

Forward Direction: $P \implies Q$

Let us re-express any number n as a function of its digits. We know that the number will thus have the following value, for some k-digit number.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1}$$

We know that since 10^2 is divisible by 4, $10^2 n_2$ is divisible by 4 for all possible values of n_2. This is true for all $n_3, \ldots, n_{k-1}$. Since the number formed by the first two digits $n_0 + 10n_1$ is divisible by 4, n is divisible by 4.

Reverse Direction: $Q \implies P$

If n is divisible by 4, we can re-express $n = 4l$ for some integer l. We wish to prove that this implies the last two digits are divisible by 4. We see

$$n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1} = 4l.$$

Re-arrange, and we have

$$\frac{n_0+10n_1}{4}+25n_2+250n_3+\cdots+25\cdot 10^{k-3}n_{k-1}=l.$$

Since l is an integer, and all values after the first two terms are integers, we have that $(n_0+10n_1)/4$ is necessarily an integer. This implies that 4 divides n_0+10n_1.

(b) We will again use modular arithmetic to prove both directions of the implication at once. We will show that the condition that n is divisible by 3 is equivalent to condition that the sum of n's digits is divisible by 3.

Consider the following expression for n.

$$n=\sum_{i=0}^{k-1}10^i n_i \pmod 3$$

Note that in mod 3, $10=1$, so in mod 3, this is equivalent to

$$n\equiv\sum_{i=0}^{k-1}n_i \pmod 3.$$

As it turns out, the latter expression is exactly the sum of all the digits in n. As a result, n is 0 in mod 3 if and only if the sum of all the digits is 0 in mod 3.

4 Just Can't Wait

Joel lives in Berkeley. He mainly commutes by public transport, i.e., bus and BART. He hates waiting while transferring, and he usually plans his trip so that he can get on his next vehicle immediately after he gets off the previous one (zero transfer time, i.e. if he gets off his previous vehicle at 7:00am he gets on his next vehicle at 7:00am). Tomorrow, Joel needs to take an AC Transit bus from his home stop to the Downtown Berkeley BART station, then take BART into San Francisco.

(a) The bus arrives at Joel's home stop every 22 minutes from 6:05am onwards, and it takes 10 minutes to get to the Downtown Berkeley BART station. The train arrives at the station every 8 minutes from 4:25am onwards. What time is the earliest bus he can take to be able to transfer to the train immediately? Show your work. (Find the answer without listing all the schedules. Hint: derive an equation relating the bus number and train number and then work in modular arithmetic to get rid of one of the variables to give a set of possible train numbers.)

(b) Joel has to take a Muni bus after he gets off the train in San Francisco. The commute time on BART is 33 minutes, and the Muni bus arrives at the San Francisco BART station every 17 minutes from 7:12am onwards. What time is the earliest bus he could take from Berkeley to ensure zero transfer time for both transfers? If all bus/BART services stop just before midnight, is it the only bus he can take that day? Show your work.

Solution:

(a) The earliest AC Transit bus Joel can take is at 7:11am, from which he can transfer to BART immediately after he gets off the bus at 7:21am.

Let the x^{th} bus (zero-based) be the bus Joel can take with zero transfer time, and let the y^{th} train (zero-based) be the train that he will connect to. Taking the time the BART starts running (4:25am) as a reference point, let t be the time in minutes from 4:25am to the transfer time to the y^{th} train [1]. Figure 1 shows the timeline.

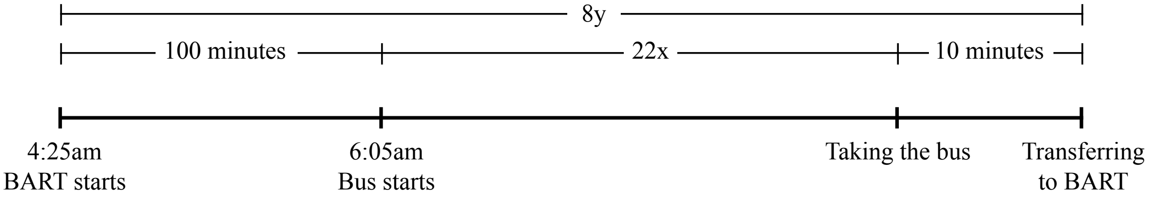

Figure 1: Timeline

From the timeline, we see the relation between x, y, and t,

$$\begin{aligned} t = 100 + 22x + 10 &= 8y \\ 8y - 22x &= 110 \\ 4y - 11x &= 55 \end{aligned} \tag{1}$$

We modulo both sides of Equation (1) with 11 to eliminate x,

$$\begin{aligned} &\text{Left-hand side: } (4y - 11x) \equiv 4y, \quad (\text{mod } 11), \\ &\text{Right-hand side: } 55 \equiv 0 \quad (\text{mod } 11), \end{aligned}$$

and form a congruence,

$$4y \equiv 0 \pmod{11}. \tag{2}$$

Since 3 is the multiplicative inverse of 4 modulo 11. Multiplying both sides of the congruence (2) by 3 gives us y,

$$\begin{aligned} 3 \cdot 4y &\equiv 3 \cdot 0 \pmod{11} \\ y &\equiv 0 \pmod{11}, \\ y &\in \{\dots, 0, 11, 22, 33, \dots\}. \end{aligned}$$

Since the bus hasn't started running when the 0^{th} and 11^{th} trains run, the 22^{th} train is the first train to connect to. The 22^{th} train departs at 4:25am + 8(22) minutes = 4:25am + 2:56 hours = 7:21am. The bus that arrives the BART station at 7:21am departs Joel's home stop at 7:21am - 10 minutes = 7:11am.

[1] Using any other time as a reference point works too, i.e., midnight, 7:00am (and find the BART departure after 7:00am), etc.

(b) The first AC Transit bus Joel can take is at 11:35am, from which he can connect to BART at 11:45am, and then Muni bus at 12:18pm. This is the only bus of the day that he can avoid waiting for both transfers.

From part a, we know that the soonest time Joel can arrive the San Francisco BART station is 7:21am + 33 minutes = 7:54am, and that he can choose to arrive every 88 minutes after that, since it is the interval AC Transit bus and BART coincides again. Let x be the number of times this 88-minute interval occurs after 7:54am (x starts from 0), and y^{th} bus (zero-based) be the Muni bus that Joel can transfer to with zero transfer time. Taking the time the Muni bus starts running (7:12am) as a reference point, let t be the time in minutes from 7:12am to the transfer time from BART to the y^{th} Muni bus. Figure 2 shows the timeline.

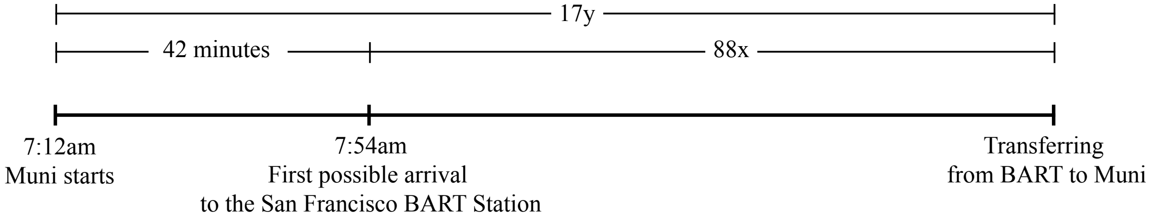

Figure 2: Timeline

Again, we write a relation between x, y, and t.

$$\begin{aligned} t = 42 + 88x &= 17y \\ 17y - 88x &= 42 \qquad (3) \end{aligned}$$

The rest is quite similar to part a.

We modulo both sides of Equation (3) with 88 to eliminate x and form a congruence,

$$17y \equiv 42 \pmod{88}. \qquad (4)$$

We have $17 \times 5 = 85 \equiv -3 \pmod{88}$. Let's mutiply both sides by 5:

$$-3y \equiv 210 \equiv 34 \pmod{88}. \qquad (5)$$

We have $3 \times 29 = 87 \equiv -1 \pmod{88}$. Let's mutiply both sides by 29:

$$\begin{aligned} y &\equiv 34 \times 29 = 986 \equiv 18 \pmod{88}, \qquad (6) \\ y &\in \{\dots, -70, 18, 106, \dots\}. \qquad (7) \end{aligned}$$

The first Muni bus Joel can take with zero transfer time is the 18th Muni bus at 7:12am + 17(18) minutes = 7:12am + 5:06 hours = 12:18pm. Subtracting the 33 minutes BART transit time, the BART departure time is 12:18pm - 33 minutes = 11:45am. Subtracting the 10 minutes AC Transit travel time, the AC Transit bus departure time is 11:45am - 10 minutes = 11:35am.

Because the Least Common Multiple of 88 and 17 is $88 \times 17 = 1496$, it will take 1,496 minutes = 24 hours 56 minutes for all three buses and BART to coincide again. Since all services stop just before midnight and restart at their respective times the next day, all three buses and BART coincide only once a day, and what we found is the only bus Joel can take that day. □

5 Fermat's Little Theorem

Fermat's Little Theorem states that for any prime p and any $a \in \{1,2,\dots,p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

Solution:

Let $n \in \mathbb{N}$. We begin by breaking down 42 into prime factors: $42 = 7 \times 3 \times 2$. Since 7, 3, and 2 are prime, we can apply Fermat's Little Theorem, which says that $a^p \equiv a \pmod{p}$, to get the congruences

$$n^7 \equiv n \pmod{7}, \tag{8}$$
$$n^3 \equiv n \pmod{3}, \qquad \text{and} \tag{9}$$
$$n^2 \equiv n \pmod{2}. \tag{10}$$

Now, let's take (9) and multiply it by $n^3 \cdot n$. This gives us

$$n^7 \equiv n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \pmod{3},$$

and since by (9), $n^3 \equiv n \pmod{3}$, this gives

$$n^7 \equiv n \pmod{3}.$$

Similarly, we take (10) and multiply by $n^2 \cdot n^2 \cdot n$ to get

$$n^7 \equiv n^2 \cdot n^2 \cdot n^2 \cdot n \equiv n^4 \pmod{2}.$$

Notice that $n^4 \equiv n^2 \cdot n^2 \equiv n \cdot n \equiv n^2 \pmod{2}$, and by (10) $n^2 \equiv n \pmod{2}$, so we have

$$n^7 \equiv n \pmod{2}.$$

Thus,

$$n^7 \equiv n \pmod{7}, \tag{11}$$
$$n^7 \equiv n \pmod{3}, \qquad \text{and} \tag{12}$$
$$n^7 \equiv n \pmod{2}. \tag{13}$$

Let $x = n^7 - n$. By the Chinese Remainder Theorem, the system of congruences

$$x \equiv 0 \pmod{7}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 0 \pmod{2}$$

has a unique solution modulo $2 \cdot 3 \cdot 7 = 42$, and this unique solution is $x \equiv 0 \pmod{42}$. So, we have that $n^7 - n \equiv 0 \pmod{42}$, which means $n^7 - n$ is divisible by 42.

6 Sparsity of Primes

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: this is a Chinese Remainder Theorem problem. We want to find x such that $x+1;x+2;x+3;$ $: : :x+k$ are all not powers of primes. We can enforce this by saying that $x+1$ through $x+k$ each must have two distinct prime divisors.

Solution:

We want to find x such that $x+1, x+2, x+3, \dots x+k$ are all not powers of primes. We can enforce this by saying that $x+1$ through $x+k$ each must have two distinct prime divisors. So, select $2k$ primes, $p_1, p_2, \dots, p_{2k}$, and enforce the constraints

$$\begin{aligned}
x+1 &\equiv 0 \pmod{p_1 p_2} \\
x+2 &\equiv 0 \pmod{p_3 p_4} \\
&\vdots \\
x+i &\equiv 0 \pmod{p_{2i-1} p_{2i}} \\
&\vdots \\
x+k &\equiv 0 \pmod{p_{2k-1} p_{2k}}
\end{aligned}$$

By Chinese Remainder Theorem, we can calculate the value of x so this x must exist, and thus, $x+1$ through $x+k$ are not prime powers.

What's even more interesting here is that we could select any $2k$ primes we want!

7 Unique Prime Factorization

We proved in lecture that every positive integer has a factorization into primes. Using the techniques in this course, we can show that this factorization is unique, up to reordering the factors!

Recall from lecture that we defined a prime number p to be a positive integer whose only positive factors are 1 and p.

In this problem, you should not assume that the positive integers have unique prime factorization.

(a) Let p and q be distinct primes. Show that $p \nmid q$.

(b) Prove that if a and b are positive integers such that $p \mid ab$, then $p \mid a$ or $p \mid b$. (Hint: Use the Extended Euclidean algorithm: There are integers x, y such that $ax + py = \gcd(a, p)$.)

(c) Show that the prime factorization of a positive integer n is unique up to reordering the factors. (Hint: Suppose that there were two prime factorizations of n. Use the previous parts to show that the factorizations are the same.)

Solution:

(a) Suppose for contradiction that $p \mid q$. Then there is some (positive) integer k such that $q = kp$. First, we note that $k \neq q$, as $p \neq 1$. Then $k > 1$ (with $k \neq p$, then q would have a factor > 1 that is not q, which is not possible. Thus, we must have $k = 1$, so $q = p$, which is a contradiction. We conclude that $p \nmid q$.

(b) By the extended Euclidean Algorithm, there are integers x, y such that

$$ax + py = \gcd(a, p).$$

If $p \mid a$, then we are done. Thus, suppose $p \nmid a$. Then p is not a factor of a, so $\gcd(a, p) = 1$, as the only other factor of p is 1. Thus, we have integers x, y such that

$$ax + py = 1.$$

Multiplying both sides by b gives that

$$abx + pby = b.$$

Since $p \mid ab$, $p \mid abx + pby$. Thus, $p \mid b$, as desired.

(c) Suppose n had two prime factorizations $p_1 \cdots p_r$ and $q_1 \cdots q_s$. We need to show that $r = s$, and the q_i are some reordering of the p_i.

Since p_1 divides the first factorization, it must divide the second factorzation. By part (b), p_1 must divide q_j for some j, and by part (a), we conclude that $p_1 = q_j$. We can thus divide both sides by p_1.

We inductively continue divide off factors of p_i. If $r < s$ or $s > r$, we get in the end that 1 is a product of primes, which is not possible. Thus, we must have $r = s$. Moreover, our inductive process shows that the q_i are the same primes as the p_i, except possibly reordered, as desired.

8 Wilson's Theorem

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \ldots \cdot p-1$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod q$?

Solution:

Direction 1: If p is prime, then the statement holds.

For the integers $1,\cdots,p-1$, every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when $x^2 \equiv 1 \pmod p$, or when $p \mid x^2-1=(x-1)(x+1)$. Thus, $p \mid x-1$ or $p \mid x+1$, so $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$. Thus, the only integers from 1 to $p-1$ inclusive whose inverse is the same as itself are 1 and $p-1$.

We reconsider the product $(p-1)! = 1 \cdot 2 \cdots p-1$. The product consists of 1, $p-1$, and pairs of numbers with their inverse, of which there are $\frac{p-1-2}{2} = \frac{p-3}{2}$. The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \equiv -1 \pmod p$, as desired.

Direction 2: The expression holds *only if* p is prime (contrapositive: if p isn't prime, then it doesn't hold).

We will prove by contradiction that if some number p is composite, then $(p-1)! \not\equiv -1 \pmod p$; Hypothetically assume that $(p-1)! \equiv -1 \pmod p$. Note that this means we can write $(p-1)!$ as $p*k-1$ for some integer k.

Since p isn't prime, it has some prime factor q where $2 \leq q \leq n-2$, and we can write $p = q*r$. Plug this into the expression for $(p-1)!$ above, yielding us $(p-1)! = (q*r)k-1 = q(rk)-1 \implies (p-1)! \equiv -1 \pmod q$. However, we know q is a term in $(p-1)!$, so $(p-1)! \equiv 0 \pmod q$. Since $0 \not\equiv 1 \pmod q$, we have reached our contradiction.