CS 70 Discrete Mathematics and Probability Theory
Fall 2019 Alistair Sinclair and Yun S. Song

HW 4

Note: *This homework consists of two parts. The first part (questions 1-6) will be graded and will determine your score for this homework. The second part (questions 7-8) will be graded if you submit them, but will not affect your homework score in any way. You are strongly advised to attempt all the questions in the first part. You should attempt the problems in the second part only if you are interested and have time to spare.*

For each problem, justify all your answers unless otherwise specified.

Part 1: Required Problems

1 The Last Digit

In each case show your work and justify your answers.

(a) If $9k+5$ and $2k+1$ have the same last digit for some natural number k, find the last digit of k.

(b) If $S = \sum_{i=1}^{19} i!$, then find the last digit of S^2.

(c) Denote the last digit of a natural number a by b. Show that the last digit of a^n is the same as the last digit of b^n where is $n \geq 1$ is a natural number.

(d) Inspired by part (c), show that the last digit of a^{4k+1} for all natural numbers k is the same as the last digit of a. [Euler's Theorem is not allowed.]

Solution:

(a) We have

$$\begin{aligned} 9k+5 &\equiv 2k+1 \pmod{10}, \\ 7k &\equiv -4 \pmod{10}, \\ 7k &\equiv 6 \pmod{10}. \end{aligned}$$

Now since gcd(7,10)=1, 7 has a (unique) inverse mod 10, and since $7 \times 3 = 21 \equiv 1 \pmod{10}$ the inverse is 3. We multiply both sides of $7k \equiv 6 \pmod{10}$ by 3:

$$k \equiv 18 \equiv 8 \pmod{10}.$$

Hence, the last digit of k is 8.

(b) Note that for $n \geq 5$:

$$n! = \left(\prod_{i=6}^{n} i\right) \times 5! = \left(\prod_{i=6}^{n} i\right) \times 120 \equiv 0 \pmod{10}.$$

So we have:

$$S = \sum_{i=1}^{19} i! = 1! + 2! + 3! + 4! + \sum_{i=5}^{19} i! = 1 + 2 + 6 + 24 + 0 \equiv 3 + 0 \pmod{10}.$$

Then, for S^2:

$$S^2 \equiv 9 \pmod{10}.$$

Hence, the last digit of S^2 is 9.

(c) By definition we have:

$$a \equiv b \pmod{10}.$$

From Theorem 6.1 we have: $a \times a \equiv b \times b \pmod{m}$. If we repeat this $n-1$ times then we get:

$$a^n \equiv b^n \pmod{10}.$$

Thus, the last digit of a^n is the same as the last digit of b^n.

(d) Since we only need the last digit of a to determine the last digit of a^n, we investigate this for all possible last digits of b, i.e. $\{0,1,2,3,4,5,6,7,8,9\}$, when they are raised to the power n.

b	0	1	2	3	4	5	6	7	8	9
$b^2 \pmod{10}$	0	1	4	9	6	5	6	9	4	1
$b^3 \pmod{10}$	0	1	8	7	4	5	6	3	2	9
$b^4 \pmod{10}$	0	1	6	1	6	5	6	1	6	1
$b^5 \pmod{10}$	0	1	2	3	4	5	6	7	8	9

As we can see for b^5 we get the same last digit as b. As a result, b^6 is the same as b^2, b^7 is the same as b^3, and so on.

Hence, for any natural number k, and $0 \leq \ell \leq 3$, $b^{4k+\ell} \equiv b^{\ell} \pmod{10}$.

So for $\ell = 1$:

$$b \equiv b^{4k+1} \pmod{10}.$$

And from part (c) we conclude:

$$a \equiv a^{4k+1} \pmod{10},$$

where b is the last digit of a.

2 Modular Arithmetic Problems

In each case show your work and justify your answers.

(a) For natural numbers a, show that $7a+3$ and $5a+2$ are coprime.

(b) What is $3^{48} \pmod{11}$?

(c) Solve $x^2+x \equiv 2 \pmod{4}$.

(d) If $17x^{12}+5x^7-14x^{40} \equiv 6 \pmod{7}$, find x.

(e) If $a+4c \equiv 2b \pmod{21}$, simplify $100a+10b+c \pmod{21}$.

In parts (c), (d), and (e) give your solutions as integers mod m.

Solution:

(a) Let $x = 7a+3$ and $y = 5a+2$. We want to show that $\gcd(x,y) = 1$, i.e. x and y are coprime. We use Euclid's Algorithm.

$$\begin{aligned}
\gcd(x,y) &= \gcd(7a+3, 5a+2) \\
&= \gcd(5a+2, 7a+3-(5a+2)) \\
&= \gcd(5a+2, 2a+1) \\
&= \gcd(2a+1, 5a+2-2(2a+1)) \\
&= \gcd(2a+1, a) \\
&= \gcd(a, 2a+1-2a) \\
&= \gcd(a,1) = 1.
\end{aligned}$$

So $\gcd(7a+3, 5a+2) = 1$. Hence, $7a+3$ and $5a+2$ are coprime.

(b) According to Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$ where $gcd(a,p) = 1$. So $3^{10} \equiv 1 \pmod{11}$. Then,

$$3^{48} = \left(3^{10}\right)^4 \cdot 3^8 \equiv (1) \cdot 3^8 = \left(3^2\right)^4 \equiv (-2)^4 = 16 \equiv 5 \pmod{11}.$$

Alternatively,

$$3^{48} = \left(3^{10}\right)^4 \cdot 3^8 \equiv (1) \cdot 3^8 = \left(3^4\right)^2 \equiv (81)^2 \equiv (4)^2 = 16 \equiv 5 \pmod{11}.$$

Thus, $3^{48} \equiv 5 \pmod{11}$.

(c)

$$x^2+x \equiv 2 \pmod{4} \Rightarrow x^2+x-2 \equiv (x+2)(x-1) \equiv 0 \pmod{4}.$$

So we have two possible solutions for x:

$$x+2 \equiv 0 \pmod 4 \Rightarrow \quad x \equiv 2 \pmod 4,$$
$$x-1 \equiv 0 \pmod 4 \Rightarrow \quad x \equiv 1 \pmod 4.$$

Hence, the solution is $x \equiv 2 \pmod 4$ or $x \equiv 1 \pmod 4$.

Note that it is not possible to set $(x+2) = 2$ and $(x-1) = 2$ in order to have $(x+2)(x-1) = 4 \equiv 0 \pmod 4$ since we should have $x = 0$ and $x = 3$ at the same time which is a contradiction.

(d) Fermat's little theorem states that if p is a prime number, then for any integer x, the number $x^p - x$ is an integer multiple of p. So

$$x^7 \equiv x \pmod 7.$$

We use this in $17x^{12} + 5x^7 - 14x^{40} \equiv 6 \pmod 7$.

$$\begin{aligned} 17x^{12} + 5x^7 - 14x^{40} &\equiv 17x^7 \cdot x^5 + 5x - (0)x^{40} \pmod 7 \\ &\equiv 17x^6 + 5x \equiv 6 \pmod 7. \end{aligned}$$

So

$$17x^6 + 5x \equiv 6 \pmod 7.$$

Here x cannot be divisible by 7, otherwise $17x^6 + 5x \equiv 0 \pmod 7$. Hence, from Fermat's Little theorem:

$$x^{p-1} \equiv 1 \pmod p.$$

Hence,

$$x^6 \equiv 1 \pmod 7.$$

So

$$17x^6 + 5x \equiv 17 \cdot 1^6 + 5x \equiv 6 \pmod 7.$$

$$\Rightarrow 5x \equiv 6 - 17 \equiv 3 \pmod 7.$$

Now since gcd(5,7)=1, 5 has a (unique) inverse mod 7, and since $5 \times 3 = 15 \equiv 1 \pmod 7$ the inverse is 3. We multiply both sides of $5x \equiv 3 \pmod 7$ by 3.

$$x \equiv 9 \equiv 2 \pmod 7.$$

(e) We know $a + 4c \equiv 2b \pmod{21}$. To simplify we write:

$$100a + 10b + c = 100a + 5(2b) + c \pmod{21}.$$

We can replace $2b$ from the assumption in the question:

$$100a + 5(a + 4c) + c = 105a + 21c = 21(5a + c) \equiv 0 \pmod{21}.$$

Hence,

$$100a + 10b + c \equiv 0 \pmod{21}.$$

3 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 you *switch* any two digits in an ISBN and still have it be a valid ISBN? For example, could 012345678X and 015342678X both be valid ISBNs? Explain.

Solution:

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

4 Product of Two

Suppose that $p > 2$ is a prime number and S is a set of numbers between 1 and $p-1$ such that $|S| > p/2$, i.e. $(\forall x \in S)(1 \leq x \leq p-1)$. Prove that any number $1 \leq x \leq p-1$ can be written as the product of two (not necessarily distinct) numbers in S, mod p.

Solution:

Given x, consider the set T defined as $\{xy^{-1} \pmod{p} : y \in S\}$. Note that the set T has the same cardinality as S, because for $y_1 \neq y_2 \pmod{p}$, we have $xy_1^{-1} \neq xy_2^{-1} \pmod{p}$ (if not, we can multiply both sides by x^{-1}, and take the inverse to get a contradiction).

Therefore, the sets S and T must have a non-empty intersection. So there must be $y_1, y_2 \in S$ such that $xy_1^{-1} = y_2 \pmod{p}$. But this means that $x \equiv y_1 y_2 \pmod{p}$.

5 RSA with Just One Prime

Given the message $x \in \{0, 1, \ldots, N-1\}$ and $N = pq$, where p and q are prime numbers, conventional RSA encrypts x with $y = E(x) \equiv x^e \pmod{N}$. The decryption is done by $D(y) \equiv y^d \pmod{N}$, where d is the inverse of $e \pmod{(p-1)(q-1)}$.

Alice is trying to send a message to Bob, and as usual, Eve is trying to decipher what the message is. One day, Bob gets lazy and tells Alice that he will now use $N = p$, where p is a 1024-bit prime number, as part of his public key. He tells Alice that it's okay, since Eve will have to try out 2^{1024} combinations to guess x. It is very likely that Eve will not find out the secret message in a reasonable amount of time! In this problem, we will see whether Bob is right or wrong. Assume that Eve has found out about this new setup and that she knows the public key.

Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{p}$, and $D(y) \equiv y^d \pmod{p}$. Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.

(a) Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve compute d in the decryption function? If so, by what algorithm and approximately how many iterations does it take for it to terminate?

(c) Given part (b), how would Eve recover x and what algorithm would she use? Approximately how many iterations does it take to terminate?

(d) Based on the previous parts, can Eve recover the original message in a reasonable amount of time? Explain.

Solution:

(a) We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$. In other words, $x^{ed} \equiv x \pmod{p}$ $\forall x \in \{0, 1, \ldots, N-1\}$.
Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1)+1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

- x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod{p}$.
- x is not a multiple of p: Then $x^{ed} \equiv x^{k(p-1)+1} \equiv x^{k(p-1)}x \equiv 1^k x \equiv x \pmod{p}$, by using FLT.

And for both cases, we have shown that x is recovered by $E(D(y))$.

(b) Since Eve knows the value of $N = p$, and the fact that $d \equiv e^{-1} \pmod{p-1}$, she can compute d using EGCD. Since EGCD decreases the largest number by at least a factor of two every two iterations, Eve needs at most $2n$ iterations, where n is the number of bits of the larger input. This means at most 2048 iterations.

(c) Since Eve now has d from part 3, and the encrypted message y, she can calculate x directly by using $D(y) = x \equiv y^d \pmod{p}$. She can now use exponentiation by repeated squaring, giving her no more than 1024 iterations.

(d) Assuming each recursive call in EGCD and exponentiation by squaring have reasonable operation time costs, Eve only needs at most 3×1024 iterations, which can easily be done with today's computing power.

6 RSA for Midterm Scores

Alice wants to tell Bob her midterm score, m, which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know her midterm score.

(a) Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's midterm score is. How did she do it?

(b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm, encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r. How can she figure out m?

Solution:

(a) There are only 101 possible values for Alice's score, so Eve can try encrypting all 101 values with Bob's public key and find out which one matches the one Alice sent.

(b) Alice sends $x = r^e \pmod{pq}$, as well as $y = (rm)^e = r^e m^e = xm^e \pmod{pq}$. We can find $x^{-1} \pmod{N}$ using the Extended Euclidean Algorithm, and multiplying this value by y gives us $m^e \pmod{N}$. Now we proceed as in the previous part to find m.

Note: *This concludes the first part of the homework. The problems below are optional, will not affect your score, and should be attempted only if you have time to spare.*

Part 2: Optional Problems

7 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.)

(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.

[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.

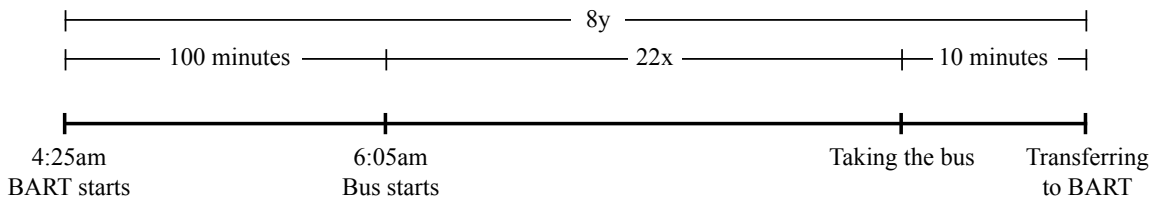

Figure 1: Timeline

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,

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

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,

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

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.

(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

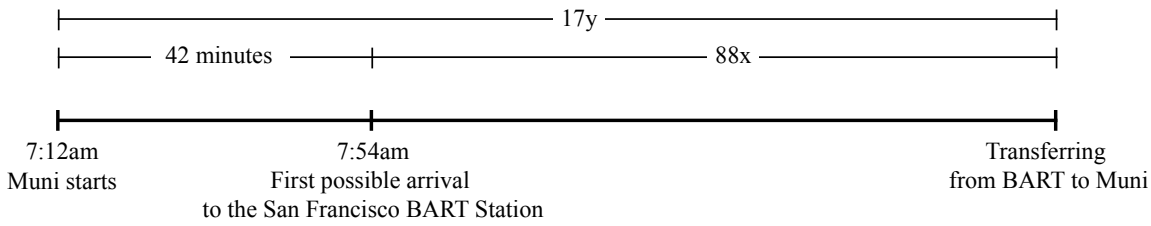

Figure 2: Timeline

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.

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

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

The rest is quite similar to part a.

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

$$17y \equiv 42 \pmod{88}. \tag{4}$$

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

$$-3y \equiv 210 \equiv 34 \pmod{88}. \tag{5}$$

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

$$y \equiv 34 \times 29 = 986 \equiv 18 \pmod{88}, \tag{6}$$

$$y \in \{\ldots, -70, 18, 106, \ldots\}. \tag{7}$$

The first Muni bus Joel can take with zero transfer time is the 18^{th} 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. □

8 Quantum Factoring

We're pretty sure that classical computers can't break RSA (because it is hard to factor large numbers on them), but we know that quantum computers theoretically could. In this question, we

will prove a fact that is a key part of Shor's Algorithm, a quantum algorithm for factoring large numbers quickly[2].

Let $N = pq$ where p, q are primes throughout this question.

(a) Prove that, for all $a \in \mathbb{N}$, there are only four possible values for $gcd(a, N)$.

(b) Using part (a), prove that, if $r^2 \equiv 1 \mod N$ and $r \not\equiv \pm 1 \pmod N$ (i.e. r is a "nontrivial square root of 1" mod N), then $gcd(r-1, N)$ is one of the prime factors of N.
Hint: $r^2 = 1 \mod N$ can be rewritten as $r^2 - 1 = 0 \mod N$ or $(r+1)(r-1) = 0 \mod N$.

Solution:

(a) N only has four divisors: 1, p, q, and N. $gcd(a, N)$ is a divisor of N, and can thus only take one of those four values.

(b) Since we are restricted to four possible values, this is conducive to a proof by cases. We only have to show that $gcd(r-1, N)$ is not 1 or N; $gcd(r-1, N)$ can only take one of the previous four values, and, if it is not 1 or N, then it must be one of the prime factors.

Case 1: Proving $gcd(r-1, N) \neq 1$:

Assume for the sake of contradiction that $gcd(r-1, N) = 1$. By the extended GCD algorithm, $gcd(r-1, N) = a(r-1) + bN$. Since $bN \equiv 0 \pmod N$, then:

$$\begin{aligned} a(r-1) &\equiv 1 \pmod N \\ a(r^2-1) &\equiv r+1 \pmod N \end{aligned} \tag{8}$$

where the second line comes from multiplying both sides by $(r+1)$. We know the left side is 0 since $r^2 - 1 \equiv 0 \pmod N$, but this implies $0 \equiv r+1 \mod N$, or $r \equiv -1 \mod N$. Since we assumed that r is a nontrivial square root of 1, this is a contradiction.

Case 2: Proving $gcd(r-1, N) \neq N$:

If $gcd(r-1, N) = N$, then $N | r-1$ and therefore $r - 1 \equiv 0 \pmod N$. Therefore $r = 1 \pmod N$. However, we assumed that r is a nontrivial square root of 1, so this is a contradiction.

Since $gcd(r-1, N) \neq 1$ and $gcd(r-1, N) \neq N$, $gcd(r-1, N)$ must be one of the prime factors of N.

[2]Read more at `https://en.wikipedia.org/wiki/Shors_algorithm`.