HW 5

Anthony Kolotv

3/8/25

Suppose that a and b are integers, $a \equiv 13 \pmod{19}$, and $b \equiv 5 \pmod{19}$. Find the integer c such that $0 \leq c \leq 18$ (i.e., $c \in \mathbb{Z}_{19}$) satisfying:

1. $c \equiv 13a \pmod{19}$

   13 × 13 = 169/19 = 8.89 (round down)

   169 - (8 × 19) = 169 - 152 = 17 = c

2. $c \equiv 8b \pmod{19}$

   8 × 5 = 40 (mod 19), 40/19 = R2

   40 - 2 × 19 = 40 - 38 = 2 = c

3. $c \equiv a - 2b \pmod{19}$

   13 - 2(5) = 3 (mod 19) = c

4. $c \equiv 7a + 3b \pmod{19}$

   7 × 13 + 3 × 5 = 91+15 = 106

   106/19 = 5.57, 106 - (5 × 19) = 11 = c

5. $c \equiv 2a^2 + 3b^2 \pmod{19}$

   $2(13^2) + 3(5^2) = 338 + 75 = 413$

   413 / 19 = 21.74, 413 - (21 × 19) = 14 = c

6. $c \equiv a^3 + 4b^3 \pmod{19}$

   $13^3 + 4\ (5^3) = 2697$

   2697/19 = 141.9, 2697 - (141 × 19) = 18 = c

Evaluate the following congruence's:

1. $-101 \pmod{11}$

   -101 / 11 = 9.18, 101 - (9 × 11) = 2

   101 ≡ 2 (mod 11) | since we started with -101, we take the neg:

   -101 ≡ -2 (mod 11) | -2+11 = 9 | get positive remainder

   -101 ≡ 9 (mod 11)

2. $(-3)^{100} \pmod{24}$

   -3 + 24 = 21 | positive equivalent

   $21^{100} \pmod{24}$

   21^2 = 441, 441/24 = 18, 441 -(18 × 24) = 9

   21^3 = 9,261, 9261/24 = 385, 9261 -(365 × 24) = 21

   if you continue - there will be a repeating pattern with even numbers having remainder 9 and odd numbers remainder 21

   since 2 is even and 100 is even, $\therefore -3^{100} \pmod{24} = 9$

3. $(185 \pmod{23})^2 \pmod{31}$

   185 / 23 = 8, 185 - (8 $\times$ 23) = 185-184=1

   $1^2 = 1$, $1 \pmod{31} = 1$

Convert each of the following binary expansions into decimal, octal, and hexadecimal expansions. Show your steps.

1. $(1000000001)_2$

   Decimal $= (1 \times 2^9) + (1 \times 2^0) = (513)_{10}$

   Octal = 1 000 000 001 = $(1001)_8$

   Hexadecimal = [00]10 0000 0001 = $(201)_{16}$

2. $(110100100010000)_2$

   Decimal $= (1 \times 2^{14}) + (1 \times 2^{13}) + (1 \times 2^{11}) + (1 \times 2^8) + (1 \times 2^4) = (26896)_{10}$

   Octal = 110 100 100 010 000 = 64420_8

   Hexadecimal = 110 1001 0001 0000 = 6910_{16}

Convert the decimal numbers 4077 and 6643 into binary, octal, and hexadecimal expansions. Show your steps.
6643

1. Divide by 2 until you reach 0, any remainders during division process are counted as bits.
   Binary = 6643/2 = 3321 (1), 3321/2 = 1660 (1), 1660/2 = 830 (1), 830/2 = 415 (1), 415/2 = 207 (1), 130/2 = 51 (1), 51/2 = 25 (1), 25 / 2 = 12 (1), 12/2 = 6 (0), 6/2 = 3 (0)

   1100111110011

2. Divide by 8 until you reach 0, remainders are counted in reverse order.
   Octal = 6643/8 = 830 R3, 830/8 = 103 R6, 103/8 = 12 R7, 12/8 = 1 R4, 1/8 = 0 R1

   14763

3. Divide by 16 until you reach 0, remainders are counted in reverse order (use modulus).
   Hexadecimal = 6643/16 = 415 R3, 415/16 = 25 R15, 25/16 = 1 R9 1/16 = 0 R1

   = 3 15 9 1 $\rightarrow$ 1 9 15 3 $\rightarrow$ 19F3

4077

1. Binary = 4077/2 = 2038 (1), 2038/2 = 1019 (0), 1019/2 = 509 (1), 509/2 = 254 (1), 254/2= 127 (0), 127/2 = 63 (1), 63/2 = 31 (1), 31/2=15 (1), 15/2=7 (1), 7/2 = 3 (1), 3/2 = 1 (1)

   111111101101

2. Octal = 4077/8 = 509 R5, 509/8=63 R5, 63/8=7 R7, 7/8 = 0 R7

   7755

3. Hexadecimal = 4077/16 = 254 R 13, 254/16 = 15 R14, 15/16 = 0 R 15

   13 14 15 $\rightarrow$ 15 14 13 $\rightarrow$ FED

Use the Euclidean algorithm to find:

1. $\gcd(123, 277)$

   277/123 = 2 R31 $| \gcd(123, 31)$

   123/31 = 3 *and* 123 mod 31 = R30 $| \gcd(31, 30)$

   31/30 = 1 *and* 31 mod 30 = R1 $| \gcd(30, 1)$

   30/1 = 30 *and* 31 mod 1 = R0 $| \gcd(1, 0)$

   =1

2. gcd(1529, 14038)

   14038 / 1529 = 9 R277 , 1529 / 277 = 5 R144, 277/144 = 1 R133, 144/133 = 1 R11, 133/11 = 12 R1, 11/1 = 1 R0

   =1

3. gcd(12345, 54321)

   54321 / 12345 = 4 R4941, 12345/4941 = 2 R2463, 4941/2463 = 2 R15, 2463/15 = 164 R3, 15/3= 5 R0

   = 3

4. gcd(9888, 6060)

   12

Prove that $\sqrt{7}$ is irrational.

- Assume that $\sqrt{7}$ is rational. That is, assume $\sqrt{7} = \frac{a}{b}$ where a and b are integers and $\frac{a}{b}$ is in simplest form, meaning a and b have no common factors other than 1.
- Squaring both sides, we get:
$$7 = \frac{a^2}{b^2}$$
- Multiplying both sides by b^2, we obtain:
$$7b^2 = a^2$$
- Since a^2 is divisible by 7, it follows that a must also be divisible by 7. Therefore, we can write $a = 7k$ for some integer k.
- Substituting $a = 7k$ into the equation $7b^2 = a^2$, we get:
$$7b^2 = (7k)^2$$
- Simplifying the right-hand side:
$$7b^2 = 49k^2$$
- Dividing both sides by 7:
$$b^2 = 7k^2$$
- This shows that b^2 is also divisible by 7, and therefore b must also be divisible by 7.
- However, we initially assumed that a and b had no common factors other than 1. But we have just shown that both a and b are divisible by 7, which is a contradiction.
- Therefore, our assumption that $\sqrt{7}$ is rational must be false.

Thus, $\sqrt{7}$ is irrational.

Prove that if $p_1, p_2, \ldots, p_n$ are distinct prime numbers with $p_1 = 2$ and $n > 1$, then $p_1 p_2 \cdots p_n + 1$ can be written in the form $4k + 3$ for some integer k.

all prime numbers greater than 2 are odd

since $p_1 = 2$ and $n > 1$ the product $p_1, p_2, \ldots, p_n$ can be written as:

$2 \times p_2, \ldots, p_n|$ from $p_2 \cdots$ all primes are odd, so their product is odd

let $p_2, \ldots, p_n = x$ where x is an odd integer, so $2x$. Since x is an odd integer, it can be expressed as $(2k + 1)$ for some integer k:

Thus, $2(2k + 1) = 4k + 2$

The expression $p_1, p_2, \ldots, p_n + 1$ can be written as: $(4k + 2) + 1 = 4k + 3$

Prove the following statements by mathematical induction:

1. $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

2. $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} = \left(\sum_{i=1}^{n} i\right)^2$

   Assume n=1:

   $\sum_{i=1}^{1} i^3 = \frac{1^2(1+1)^2}{4} = 1|$ Now we need to prove $n = k+1$

   $\sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3|$ using induction hypothesis..

   $\frac{k^2(k+1)^2}{4} + (k+1)^3|$ Factoring $(k+1)$ ...

   $\frac{k^2(k+1)^2+4(k+1)^3}{4}|$ Factoring $(k+1)^2$ out...

   $\frac{(k+1)^2(k^2+4(k+1))}{4} = \frac{k+1^2(k+2)^2}{4}|$ This matches the original formula for $n = k+1$

3. $\sum_{i=1}^{n} i(i!) = (n+1)! - 1$

   Assume n=1:

   $\sum_{i=1}^{1} i(i!) = (1+1)! - 1 = 1|$ Assume the formula holds for n=k+1

   $\sum_{i=1}^{k+1} i(i!) = \sum_{i=1}^{k} i(i!) + (k+1)(k+1)!|$ Using induction hypothesis...

   $(k+1)! - 1 + (k+1)(k+1)!|$ Factor $(k+1)!$

   $(k+1)!(1 + (k+1)) - 1 = (k+2)! - 1$

4. $\prod_{i=0}^{n} \left(\frac{1}{2i+1} \cdot \frac{1}{2i+2}\right) = \frac{1}{(2n+2)!}$

   assume n=0 (bc i=0, lowest valid case):

   $\prod_{i=0}^{0} \left(\frac{1}{2(0)+1} \cdot \frac{1}{2(0)+2}\right) = \frac{1}{(2(0)+2)!} = \frac{1}{2}|$ Prove that the formula holds for n=k+1

   $\prod_{i=0}^{k+1} \left(\frac{1}{2i+1} \cdot \frac{1}{2i+2}\right) = \frac{1}{(2(k+1)+2)!}|$ Expanding the right side...

   $\frac{1}{(2(k+1)+2)(2(k+1)+1)} = \frac{1}{(2k+3)(2k+4)}|$ Simplifying...

   $\frac{1}{(2n+2)!} \cdot \frac{1}{(2k+3)(2k+4)} = \frac{1}{(2k+2)!\cdot(2k+3)(2k+4)}|$

   Notice that $(2k+2)! \cdot (2k+3)(2k+4) = (2k+4)!$ because $(2k+4)!$ includes all the terms of $(2k+2)!$ plus the next two terms, $(2k+3)$ and $(2k+4)|$ Therefore...

   $\prod_{i=0}^{k+1} \left(\frac{1}{2i+1} \cdot \frac{1}{2i+2}\right) = \frac{1}{(2k+4)!}$

Suppose that we want to prove that:

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}}$$

for all positive integers n.

1. Show that the basis step works, but the inductive step fails.

   for n = 1:

   $\frac{1}{2} < \frac{1}{\sqrt{3}} \approx 0.577 = 0.5 < 0.577|$ base case holds for n=1

   Prove the formula holds for n = k+1:

   $\prod_{i=0}^{k+1} \frac{2i-1}{2i} = (\prod_{i=0}^{k} \frac{2i-1}{2i}) \cdot \frac{2k+1}{2k+2}|$ we add $\frac{2k+1}{2k+2}$ to help prove that the inequality holds for k+1.

   $(\prod_{i=0}^{k} \frac{2i-1}{2i}) \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{3k}} \cdot \frac{2k+1}{2k+2}|$ substituting back into the equation

   Now we need to show $\frac{1}{\sqrt{3k}} \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{3(k+1)}}|$ Re-write inequality...

   $\frac{2k+1}{2k+2} < \frac{\sqrt{3}}{\sqrt{3(k+1)}}|$ Simplify the right side...

$\sqrt{\frac{k}{k+1}}$| Plugging back into the inequality ...

$\frac{2k+1}{2k+2} < \sqrt{\frac{k}{k+1}}$| Now prove inequality

$(\frac{2k+1}{2k+2})^2 < \frac{k}{k+1}$| Expanding the left side...

$\frac{4k^2+4k+1}{4k^2+8k+4} < \frac{k}{k+1}$| cross multiply to clear fractions

$(4k^2+4k+1)(k+1) < 4k^2+8k+4$| Simplify...

$4k^3+4k^2-3k-3 < 0$| Analyze...

for k=1, $4^3+4^2-3-3 = 64+16-3-3 = 74 \not< 0$

Therefore, the induction step fails

2. Show that mathematical induction can be used to prove the stronger inequality:

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}}$$

for all integers $n > 1$, which, together with verification for $n = 1$, establishes the weaker inequality.

prove that formula holds for n = k+1:

$\prod_{i=1}^{k+1} \frac{2i-1}{2i} < \frac{1}{\sqrt{(3k+1)+1}}$| We can express the left side as:

$(\prod_{i=1}^{k} \frac{2i-1}{2i}) \cdot \frac{2k+1}{2k+2}$| showing the full equation...

$(\prod_{i=1}^{k} \frac{2i-1}{2i}) \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{3k+1}} \cdot \frac{2k+1}{2k+2}$| Now prove that $\frac{1}{\sqrt{3k+1}} \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{(3k+1)+1}}$ ...

$\frac{1}{\sqrt{(3k+1)+1}} = \frac{1}{\sqrt{3k+4}}$,

$\frac{1}{\sqrt{3k+1}} \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{3k+4}}$| Multiply both sides by $\sqrt{3k+1}$ and $\sqrt{3k+4}$

$\frac{2k+1}{2k+2} < \frac{\sqrt{3k+1}}{\sqrt{3k+4}}$| Square both sides and expand

$\frac{4k^2+4k+1}{4k^2+4k+8} < \frac{\sqrt{3k+1}}{\sqrt{3k+4}}$| Multiply by both denominators...

$12k^3+28k^2+19k+4 < 12k^3+28k^2+20k+4$| Subtract $12k^3+28k^2+19k+4$ from both sides...

$0 < k$

An integer sequence $\{a_0, a_1, \dots\}$ is given by $a_0 = 0$ and $a_k = 2a_{k-1}+1$ for every $k \geq 1$.

1. Calculate by hand the first 5 terms of a_k.

$a_0 = 0$

$a_1 = 2a_{1-1}+1 = 2(0)+1 = 1$

$a_2 = 2a_{2-1}+1 = 2(1)+1 = 3$

$a_3 = 2a_{3-1}+1 = 2(3)+1 = 7$

$a_4 = 2a_{4-1}+1 = 2(7)+1 = 15$

2. Guess a simple formula for a_k.

it looks exponential, and each previous term can be multiplied by 2 and adding 1. It could be re-written as $2^k - 1$

3. Prove your conjecture from part (b) by mathematical induction.

$a_k = 2^k - 1$ for k=0 we have : $a_0 = 0$ (given)

the formula gives $2^0 - 1 = 1 - 1 = 0$ so base case holds

now prove that formula holds for $k = n+1$:

$a^{n+1} = 2^{n+1} + 1$

from the relation, we know that: $a_{n+1} = 2a_n + 1$,

by inductive hypothesis, $a_n = 2^n - 1$, so:

$a_{n+1} = 2(2^n - 1) + 1$, simplifying the right side...

$a_{n+1} = 2 \cdot 2^n - 1 + 1 = 2^{n+1} - 1$

Thus, the formula holds for $k = n + 1$