Homework 4 Solutions

Question 1

Let $n = 2^{19}3^{199}$. How many distinct divisors does n have?

Solution: Any divisor of n can be written in the form $2^n 3^m$, for some $n, m \in \mathbb{Z}$ s.t. $0 \leq n \leq 19$ and $0 \leq m \leq 199$. This follows from the fundamental theorem of arithmetic.

Since we have 20 choices for n and 200 choices for m, there are a total number of $20 \cdot 200 = 4000$ options.

Also, by the fundamental theorem of arithmetic, each combination gives a distinct divisor. $\square$

Question 2

What is the ten's digit of 7^{1942}?

Solution: Ans $= 4$.

To determine the ten's digit of 7^{1942} is same as compute 7^{1942} mod 100. We observe that,

$$
\begin{aligned}
7^0 &= 1 \mod 100 \\
7^1 &= 7 \mod 100 \\
7^2 &= 49 \mod 100 \\
7^3 &= 43 \mod 100 \\
7^4 &= 1 \mod 100
\end{aligned}
$$

$1942 \mod 4 = 2$, so we know that $7^{1942} = 7^2 \mod 100 = 49$.

Question 3

Let a, b, c and r be natural numbers. For each of the statements below justify why the statement is true or disprove it by finding a counter example:

1. If $a \mod r = b \mod r$ then $a^c \mod r = b^c \mod r$.
2. If $a \mod r = b \mod r$ then $c^a \mod r = c^b \mod r$.

Solution:

1. This claim is correct. By the division algorithm, $\exists w, x, y, z \in \mathbb{Z}$ s.t. $a = wr + x$, $b = yr + z$ and $0 \leq x, z < r$. Then,

$$\begin{aligned} x &= (wr + x) \mod r \\ &= a \mod r \\ &= b \mod r \\ &= (yr + z) \mod r \\ &= z \end{aligned}$$

Which implies $x = z$. Furthermore, by the binomial theorem,

$$\begin{aligned} a^c \mod r &= (wr + x)^c \mod r \\ &= \left(\sum_{k=0}^{c} \binom{c}{k} w^k r^k x^{c-k} \right) \mod r \\ &= \left(x^c + \sum_{k=1}^{c} \binom{c}{k} w^k r^k x^{c-k} \right) \mod r \end{aligned}$$

Since every term in the summation is multiplied by r at least once, we can factor out an r:

$$\begin{aligned} &= \left(x^c + r \sum_{k=1}^{c} \binom{c}{k} w^k r^{k-1} x^{c-k} \right) \mod r \\ &= x^c \mod r \end{aligned}$$

By the same logic, we can see that $b^c \mod r = z^c \mod r$, but since $x = z$, we can conclude $b^c \mod r = z^c \mod r = x^c \mod r = a^c \mod r$.

Note: the claim can also be proved directly using the product rule, without using the binomial theorem.

So simply you can argue:

$$\begin{aligned} a^c \mod r &= (a \mod r)^c \mod r \\ &= (b \mod r)^c \mod r \\ &= b^c \mod r \end{aligned}$$

The above calculation is justified by repeated use of the product rule. (You can make this more formal by using induction, but this is not necessary: thus the brief proof above suffices.)

2. This claim is incorrect. Suppose $a = 1, b = 5, r = 4$, and $c = 2$. Then, $a \mod r = 1 \mod 4 = 5 \mod 2 = b \mod 4$, but

$$\begin{aligned} c^a \mod r &= 2 \mod 4 \\ &= 2 \end{aligned}$$

while

$$\begin{aligned} c^b \mod r &= 32 \mod 4 \\ &= 0 \end{aligned}$$

$\square$

Question 4

Let $k = 2008^2 + 2^{2008}$. Find the units digit of $k^2 + 2^k$.

(**Hint:** the units digit is just the remainder $\mod 10$. First find the units digit of k.)

Solution: Ans $= 6$.

First observe that the last digits of powers of 2 have the pattern: $2^1 = 2 \mod 10, 2^2 = 4 \mod 10, 2^3 = 8 \mod 10, 2^4 = 6 \mod 10, 2^5 = 2 \mod 10...$ We can see it forms a cycle of length 4.

Now lets' calculate $(k^2 + 2^k) \mod 10$.

$$(k^2 + 2^k) \mod 10 = \big((k \mod 10)^2 + (2^k \mod 10)\big) \mod 10.$$

We first calculate $k \mod 10$:

$$k \mod 10 = (2008^2 + 2^{2008}) \mod 10 = (2008 \mod 10)^2 + 2^{2008} \mod 10) \mod 10$$

$$= (64 + 2^4) \mod 10 = (4 + 6) \mod 10 = 0 \mod 10,$$

where we used the cycle of length 4 for $2^i \mod 10$.

So the $(k \mod 10)^2$ term is $0 \mod 10$. What about the $2^k \mod 10$ term? It depends entirely on what $k \mod 4$ is (as 4 is the cycle length in $2^i \mod 10$). But you can easily check that $k \mod 4 = (2008^2 + 2^{2008}) \mod 4 = 0$ as both 2008 and 2^{2008} are divisible by 4. Thus looking at the $2^i \mod 10$ cycle, $2^k \mod 10 = 6$. Thus, finally, $(k^2 + 2^k) \mod 10 = 6$.

Question 5

Suppose p and q are distinct primes and a is some natural number. Further, $a^p = a \mod q$ and $a^q = a \mod p$. Prove that $a^{pq} = a \mod pq$.

Solution:

$$\begin{aligned} a^{pq} \mod p &= (a^p)^q \mod p \\ &= (a^p \mod p)^q \mod p \quad \text{, by product rule} \\ &= a^q \mod p \quad \text{, by Fermat's little theorem} \\ &= a \mod p \quad \text{, by fact provided in the question} \end{aligned}$$

By an entirely similar calculation, $a^{pq} \mod q = a^p \mod q = a \mod q$. So we know that $a^{pq} - a \mod p = 0$ and also that $a^{pq} - a \mod q = 0$. Thus p and q both divide $a^{pq} - a$.

If a number is divisible by two distinct primes, then it must be divisible by their product (this follows from the Fundamental theorem of Arithmetic). Since p and q are distinct primes, hence $a^{pq} - a$ is divisible by pq and therefore $a^{pq} \mod pq = a \mod pq$.

Question 6

Prove that there is no solution in natural numbers to the equation

$$x^2 + y^2 = 3z^2.$$

(**Hint:** First show that every perfect square has a remainder of 0 or 1 when divided by 3. Now show that if there is such a solution, then there must be a “smaller" solution.)

Solution: Assume there is at least one such solution in natural numbers, and let (a, b, c) be the smallest such solution (in terms of the third number in the solution tuple). That is, let $c \neq 0$ be the smallest natural number such that $\exists a, b$, natural numbers, such that $a^2 + b^2 = 3c^2$.

Since every perfect square has a remainder of 0 or 1 when divided by 3 (you must prove this!), and $3c^2$ is a multiple of 3, thus a^2 and b^2 must both be divisible by 3 (because if you look at the equation modulo 3, it is easy to check that either of them being 1 is impossible..

Since 3 is a prime, $3|u^2 = u \cdot u$ implies $3|u$ for any natural number u (by using the fundamental theorem of arithmmetic). So a and b are also divisible by 3!

Then $a = 3a'$ and $b = 3b'$ for some $a' < a, b' < b$ where a', b' are also natural numbers.

Substituiting this into the original equation we get:

$$9(a')^2 + 9(b')^2 = 3c^2.$$

So

$$3(a')^2 + 3(b')^2 = c^2$$

and thus $3|c^2$ from which we conclude that $3|c$.

Denote $c = 3c'$ with $c' < c$ being a natural number. Again plugging in $a = 3a'$, $b = 3b'$ and $c = 3c'$ we have

$$3(a')^2 + 3(b')^2 = (3c')^2 = 9(c')^2$$

and simplifying to get

$$(a')^2 + (b')^2 = 3(c')^2$$

. However, this means that (a', b', c') and $c' < c$ is also a solution to the original equation $x^2+y^2 = 3z^2$, and $c' < c$. This contradicts our assumption that c is the smallest!

Hence there can be no natural number solution to this equation (the idea in brief being that: we proved that any natural number solution (a, b, c) implies that $(a/3, b/3, c/3)$ is also a **natural number** solution to this equation!)

Note: You can also do essentially the same proof by infinite descent, or even by induction (exercise: think carefully how you would phrase this as an inductive proof)

Finally, we used in our proof, that every perfect square is either 0 or $1 \mod 3$.

Claim: If n is a natural number, $n^2 \mod 3$ is either 0 or 1.

You can also prove this easily by using Fermat's little theorem, but here is an even simpler proof: There are only 3 possible values for $n \bmod 3$:

- $n \bmod 3 = 0 \implies n^2 \mod 3 = 0 \cdot 0 = 0 \mod 3$
- $n \bmod 3 = 1 \implies n^2 \mod 3 = 1 \cdot 1 = 1 \mod 3$
- $n \bmod 3 = 2 \implies n^2 \mod 3 = 2 \cdot 2 = 4 = 1 \mod 3$

Thus $n^2 \bmod 3 \in \{0, 1\}$.

Extra Practice Questions

Question 7

Prove that for any natural number n, $3^{2n+1} + 2^{n+2}$ is divisible by 7. (**Hint:** Use induction.)

Solution:

Base case: Let $n = 1$. Then $3^{2n+1} + 2^{n+2} = 3^3 + 2^3 = 35 \quad \checkmark$

Induction Hypothesis: Let $n = k$, $k \geq 1$. Assume $7 \mid (3^{2k+1} + 2^{k+2})$.

Induction Step: Let $n = k + 1$. Consider $3^{2n+1} + 2^{n+2} \mod 7$. We have

$$\begin{aligned} 3^{2n+1} + 2^{n+2} = 3^{2k+3} + 2^{k+3} = 3^2(3^{2k+1}) + 2(2^{k+3}) &= 2(3^{2k+1}) + 2(2^{k+3}) && \mod 7 \\ &= 2(3^{2k+1} + 2^{k+2}) && \mod 7 \\ &= 2(0) && \mod 7 \quad \text{(I.H.)} \\ &= 0 && \mod 7 \end{aligned}$$

Thus for $n = k+1$, $3^{2n+1} + 2^{n+2} = 0 \mod 7$, which implies $7 \mid (3^{2n+1} + 2^{n+2})$. This completes our proof by induction, and we have shown that $\forall n \in \mathbb{N}, 7 \mid (3^{2n+1} + 2^{n+2})$. □

Question 8

By f_n we denote the n-th Tribonacci number. Tribonacci numbers are defined by $f_1 = f_2 = 0$, $f_3 = 1$, and $f_n = f_{n-1} + f_{n-2} + f_{n-3}$ for $n \geq 4$. Thus the Tribonacci sequence goes as:

$$0, 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, \ldots$$

Prove (by induction on n) that $f_n > 3n$ for all $n > 9$.

Solution: Proceeding by strong induction. Since our recurrent relation contains three previous terms, we must consider three base cases.
Base Cases:

- For $n = 10$, $f_n = 44 > 30 = 3n$.
- For $n = 11$, $f_n = 81 > 33 = 3n$.
- For $n = 12$, $f_n = 149 > 36 = 3n$.

Inductive Hypothesis: Suppose the claim is true for all $n \leq k$ for some $k \geq 12$.
Inductive Step: Consider the case where $n = k + 1$.
Then, by the recurrence formula:

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} + f_{n-3} \\ &= f_k + f_{k-1} + f_{k-2} \end{aligned}$$

By the inductive hypothesis:

$$\begin{aligned} &> 3k + 3(k-1) + 3(k-2) \\ &= 9k - 9 \\ &= 3(k+1) + 6k - 12 \\ &= 3n + 6k - 12 \\ &\geq 3n + 6(12) - 12 \\ &> 3n \end{aligned}$$

□

Question 9

Suppose $f(n) = 2f(n/3) + n$. f is a function from natural numbers to natural numbers. Let $f(1) = 1$. Prove that $f(n) < 3n$. You may restrict your attention to the case where n is a power of 3.

Solution: We restrict our attention to the case where n is a power of 3. We will prove that for every whole number r, $f(3^r) < 3(3^r) = 3^{r+1}$, using induction on r.

Base case: Let $r = 0$. Then $f(n) = f(3^0) = f(1) = 1 < 3$ ✓

Induction Hypothesis: Let $r = k$, $k \geq 0$. Assume $f(3^k) < 3^{k+1}$.

Induction Step: Let $r = k + 1$. Then

$$\begin{aligned} f(3^r) = f(3^{k+1}) = 2f(3^{k+1}/3) + 3^{k+1} &= 2f(3^k) + 3^{k+1} \\ &< 2(3^{k+1}) + 3^{k+1} && \text{(I.H.)} \\ &= 3(3^{k+1}) \end{aligned}$$

Thus for every whole number r, $f(3^r) < 3(3^r)$. Let n be a power of 3. Then there exists a whole number r s.t. $n = 3^r$, and we have $f(n) < 3n$. $\square$

Question 10

Prove that every prime number $p > 3$, there is a natural number n such that $p = 6n + 1$ or $p = 6n - 1$.

Solution: If $p = 5$, we just let $n = 1$, so that $5 = 6 - 1$. For any prime number $p > 6$, we know that p can be written in one of the following forms: $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4, 6k + 5$, for a natural number k. Since p is prime, it cannot be written as $6k, 6k + 2, 6k + 3, 6k + 4$ because these numbers are divisible by either 2 or 3. So we know that $p = 6k + 1$ or $p = 6k + 5 = 6(k + 1) - 1$.

Question 11

There exists an infinitely large grid. You are currently at point $(1, 1)$, and you need to reach the point $(\text{targetX}, \text{targetY})$ using a finite number of steps.

In one step, you can move from point (x, y) to any one of the following points:

- $(x, y - x)$
- $(x - y, y)$
- $(2 * x, y)$
- $(x, 2 * y)$

Given two natural numbers targetX and targetY representing the X-coordinate and Y-coordinate of your final position, design a fast algorithm to return true if you can reach the point from $(1,1)$ using some number of steps, and false otherwise.

(**Hint:** The first two allowed operations should remind you of Euclid's algorithm to find the GCD of two numbers!)

Example 1:

Input: targetX $= 6$, targetY $= 9$
Output: false
Explanation: It is impossible to reach $(6,9)$ from $(1,1)$ using any sequence of moves, so false is returned.

Example 2:

Input: targetX $= 4$, target $Y = 7$
Output: true
Explanation: You can follow the path $(1,1) \to (1,2) \to (1,4) \to (1,8) \to (1,7) \to (2,7) \to (4,7)$.

Solution:

1. Compute $GCD(\text{targetX}, \text{targetY})$. This can be done in $\log(\min\{\text{targetX}, \text{targetY}\})$ time by Euclid's algorithm.
2. Return true if the GCD is a power of 2, else return false.

We are claiming that (X,Y) is reachable **if and only if** GCD(X,Y) is a power of 2. Why is this correct? We will Prove it!

Proof:

- First we claim that if $GCD(\text{targetX}, \text{targetY})$ is not a power of 2, then $(\text{targetX}, \text{targetY})$ is not reachable.

  The $GCD(1, 1) = 1$ which is power of 2. But this property is invariant under the allowed moves. The first two types of moves do not change the GCD. This is because:

  $$GCD(x, y) = GCD(x, y - x) = GCD(x - y, y)$$

  What about the other kinds of moves. Clearly all they can ever do is multiply the GCD by 2.

  Hence initially the GCD is a power of 2 and this property is invariant under the allowed set of moves. That is, whatever (x, y) you manage to reach after any sequence of these moves must have the property that $GCD(x, y)$ is a power of 2. This proves that if $GCD(\text{targetX}, \text{targetY})$ is not a power of 2, then $(\text{targetX}, \text{targetY})$ is not reachable.

- Next we claim that if $GCD(\text{targetX}, \text{targetY})$ is a power of 2, then $(\text{targetX}, \text{targetY})$ is reachable.

  Consider the reverse direction of movement. Then the question becomes, can move from $(\text{targetX}, \text{targetY})$ to $(1, 1)$, where our legal moves are from any (x, y) to $(x, x + y)$, $(x + y, y)$, $\left(\frac{x}{2}, y\right)$, or $\left(x, \frac{y}{2}\right)$? (We can only do the division by 2 type moves if the number being divided is even). If we can get from $(\text{targetX}, \text{targetY})$ to $(1, 1)$ in this way, then definitely we can go from to $(1, 1)$ to $(\text{targetX}, \text{targetY})$ using the original moves.

  As long as x or y is even, we divide it by 2 until both x and y are odd. At this point, if $x \neq y$, without loss of generality, let $x > y$, then $\frac{x+y}{2} < x$. Since $x+y$ is even, we can move from (x, y) to $(x + y, y)$, and then to $\left(\frac{x+y}{2}, y\right)$ using two moves. That is to say, we can always make x and y continuously decrease. **The only time when this process of decreasing x or y is stopped is when we hit $x = y$ and x and y are both odd.** I now claim that this can only happen when we reach (1,1).

  Why? Notice our new set of moves (the reverse direction ones) also has the same invariant: if the GCD(x, y) was a power of 2, then after any of the 4 moves, the GCD of the two numbers will remain a power of 2. So we can keep doing moves as described above, and keep reducing x and y, till eventually we hit the case of $x = y$ and both are odd. Suppose this is not the case $(1, 1)$. Say we hit a case (x, x) and x is odd but not 1. Then GCD$(x, x) = x$ which is an odd number not equal to 1, and so it is not a power of 2! But we started by saying that $GCD(\text{targetX}, \text{targetY})$ being a power of 2, and we know this property must be preserved by our moves! So this is impossible: indeed these moves will allow us to keep decreasing x and y till we get to $(1, 1)$.

  But that means that if $GCD(\text{targetX}, \text{targetY})$ is a power of 2, then the original set of moves will allow us to get to $(\text{targetX}, \text{targetY})$ from $(1, 1)$!