

1. (20) Write the negation of the following statement:

$$\forall n \in N (\exists m \in N) \wedge (\exists p \in N) \text{ such that } mn - np \notin N.$$

The negation of this statement is

$$\exists n \in N \text{ such that } (\forall m \in N) \vee (\forall p \in N) mn - np \in N$$

2. (20)

- (a) Define an equivalence relation on a set A .

An equivalence relation on a set A is a relation on A , that is, a subset of $A \times A$, which is reflexive, symmetric, and transitive.

- (b) Let R denote the following relation on the set Z of integers

$$mRn \text{ means there is a } k \in Z \text{ such that } m - 2n = 3k.$$

Determine whether or not R is an equivalence relation on Z .

R is not an equivalence relation as it is not reflexive. For example 1 is not related to itself, as $1 - 2(1) = -1$ and this is not a multiple of 3.

3. (20) Let $f : A \rightarrow B$ be a function with domain A and codomain B . Let $P(A)$ denote the power set of A .

- (a) Define what the power set of A is.

The power set of A is the set, which consists of all possible subsets of A .

- (b) Define $f : P(A) \rightarrow P(B)$.

This function takes any subset of A and maps it to its image. That is, $\forall X$ such that $X \subseteq A$

$$f(X) = \{f(x) : x \in X\} \subseteq B$$

- (c) If f is one-to-one, is $f : P(A) \rightarrow P(B)$? If yes, give a proof, if no give a counter example.

This new function is also one-to-one. For suppose $f(X_1) = f(X_2)$ for two subsets X_1 and X_2 of A . Let $x \in X_1$, then $f(x) \in f(X_1)$. Since $f(X_1) = f(X_2)$ there must be a $y \in X_2$ such that $f(x) = f(y)$. But f is one-to-one, hence $x = y$, and we see that $x \in X_2$. That is, $X_1 \subseteq X_2$. A similar argument shows that $X_2 \subseteq X_1$, and the two subsets of A are equal.

4. (20) State the Well Ordering Principle. Use it to prove that for any integers m and n , with $m > 0$, there are integers q and r , with $0 \leq r < m$ such that

$$n = qm + r .$$

The Well Ordering Principle states that if S is any nonempty subset of the positive integers, then S contains a least element.

To see that there are integers q and r with the desired properties, set

$$S = \{n - qm : q \in \mathbb{Z}, \text{ and } n - qm \geq 0\} .$$

Note: n and m are fixed, and q is any integer in \mathbb{Z} . To see that S is nonempty there are two cases to consider. The first one is if $n \geq 0$. In this case set $q = 0$. Then $n = n - 0 \cdot m \in S$. If $n < 0$, set $q = n$, then we have $n - qm = n - nm = n(1 - m)$. Since neither factor is positive ($m > 0$), their product cannot be negative so $n - qm \in S$. If $0 \in S$ we are done for then there is a q such that

$$\begin{aligned} n - qm &= 0 \text{ or} \\ n &= qm + 0 \end{aligned}$$

And we have a q and r , with $0 \leq r < m$. If $0 \notin S$. Then S is a nonempty subset of the positive integers. Let r denote its least element. Then we must have $0 \leq r$. And to see that $r < m$ suppose it isn't. Then we have

$$0 \leq r - m = n - qm - m = n - (q + 1)m < r .$$

Thus, $r - m$ is in S and smaller than the least element of S . This contradiction implies that $r < m$.

5. (20) Define the greatest common divisor of two integers m and n , where at least one of the integers m and n is non-zero. Let $d = \gcd(m, n) =$ greatest common divisor of m and n .

The greatest common divisor of m and n is a positive integer d such that

1. $d|a$ and $d|b$
2. If $c|a$ and $c|b$, then $c|d$.

- (a) Show that d is unique.

Suppose that d_1 and d_2 are both greatest common divisors of m and n . Then we must have $d_1|d_2$ and $d_2|d_1$. These statements imply there are constants k_1 and k_2 such that $d_2 = k_1d_1$ and $d_1 = k_2d_2$. Thus, we have

$$d_2 = k_1d_1 = k_1(k_2d_2) = (k_1k_2)d_2.$$

Thus, $k_1k_2 = 1$. But the only integers for which this is possible are $k = \pm 1$. If $k_1 = -1$, then $d_2 = -d_1$, which contradicts the fact that both integers must be positive. Thus, $k_1 = 1$ and $d_2 = d_1$.

- (b) Find the $\gcd(126, 516)$, and write it as a linear combination of 126 and 516.

$$\begin{aligned} 516 &= 126 \cdot 4 + 12 \\ 126 &= 12 \cdot 10 + 6 \\ 12 &= 6 \cdot 2. \end{aligned}$$

Since 6 is the last non-zero remainder, $6 = \gcd(126, 516)$, and

$$\begin{aligned} 6 &= 126 - 12(10) \\ &= 126 - 10(516 - 4 \cdot 126) \\ &= 126(41) + 516(-10) . \end{aligned}$$

6. (20) Define a prime number. Show that if p is prime and p divides the product of two integers a and b , then p must divide at least one of a and b .

A prime number is a positive integer not equal to 1 whose only divisors are itself and 1.

Suppose a prime p divides ab . If p divides a , there is nothing to prove. So suppose p does not divide a , then we must have $\gcd(a, p) = 1$. There are integers x and y such that $ax + py = 1$. Thus, we have

$$b = b(ax + py) = abx + pby.$$

Since p divides ab , we see that p divides both of the summands abx and pby . Thus, p divides their sum, which is b .

7. (15) For the Diophantine equation $ax + by = c$, where a , b , and c are integers. Show that this equation has a solution if and only if $\gcd(a, b)$ divides c . Find all solutions of the equation $42x + 172y = 6$.

First suppose that the equation $ax + by = c$ has a solution. Then if $d = \gcd(a, b)$ we have $d|ax$ and $d|by$, which implies that $d|c$, the sum of ax and by . Conversely suppose that $d|c$. Then there are integers k , x_1 and y_1 such that $c = kd$ and

$$\begin{aligned} d &= ax_1 + by_1 \\ c &= kd = k(ax_1 + by_1) \\ &= a(kx_1) + b(ky_1), \end{aligned}$$

and our Diophantine equation does indeed have a solution.

To find all solutions of $42x + 172y = 6$, we first see that $\gcd(42, 172) = 2$, which does divide 6. Since we have $2 = 42(41) + 172(-10)$, we have

$$\begin{aligned} 6 &= 42(123) + 172(-30) \\ &= 42\left(123 + \frac{172}{2}k\right) + 172\left(-30 - \frac{42}{2}k\right) \\ &= 42(123 + 86k) + 172(-30 - 21k). \end{aligned}$$

Thus, our solutions are

$$\begin{aligned} x &= 123 + 86k \\ y &= -30 - 21k, \end{aligned}$$

for any integer k .

8. (15) Determine the units digit of the number 123^{227} .

Using Fermat's Little theorem, which states that $n^p \equiv n \pmod{p}$, whenever p is a prime we have

$$\begin{aligned} 123^{227} &\equiv 1 \pmod{2} \\ 123^{227} &\equiv 3^{227} \equiv 3^{5(45)+2} \equiv 9 \cdot 3^{45} \\ &\equiv 4 \cdot 3^{5 \cdot 9} \equiv 4 \cdot 3^9 \\ &\equiv 4 \cdot 3^{5+4} \equiv 4 \cdot 3^5 \\ &\equiv 4 \cdot 3 \equiv 2 \pmod{5}. \end{aligned}$$

This equations imply

$$\begin{aligned} 5 \cdot 123^{227} &\equiv 5 \pmod{10} \\ 2 \cdot 123^{227} &\equiv 4 \pmod{10}. \end{aligned}$$

Adding the two equations together we have

$$\begin{aligned} 7 \cdot 123^{227} &\equiv 9 \pmod{10} \\ 123^{227} &\equiv 27 \pmod{10} \\ &\equiv 7 \pmod{10}. \end{aligned}$$

Thus, the units digit of 123^{227} is 7.