Chapter 00

Mostafa Touny

September 8, 2023

Contents

Problems

2(d)

Observe the prime factorization $21 = 3 \cdot 7$ and $50 = 2 \cdot 5 \cdot 5$. As they share no prime numbers, $gcd(21, 50) = 1$.

4

We have $1 = 7(-3) + 11(2) = -21 + 22$, and $1 = 7(8) + 11(-5) = 56 - 56 - 56 - 56 - 56 - 56 - 55$. Generally $1 = 7(-3 + 11k) + 11(2 - 7k)$.

7

($\rightarrow$) We are given $a = nk_0 + r$ and $b = nk_1 + r$. Thus $a - b = nk_0 - nk_1 = n(k_0 - k_1)$.

($\leftarrow$) We have $a = nk_1 + r_1$, and $b = nk_2 + r_2$. Construct $a - b = n(k_1 - k_2) + (r_1 - r_2)$ and observe we get $0 \leq r_1 - r_2 \leq n - 1$. If $r_1 - r_2 \neq 0$, Then n won't divide $a - b$ contradicting the given hypothesis.

10

We have $1 = 7(-3) + 11(2) = -21 + 22$, and $1 = 7(8) + 11(-5) = 56 - 56 - 56 - 56 - 56 - 56 - 55$. Generally $1 = 7(-3 + 11k) + 11(2 - 7k)$.

11

Observe the form $ax \mod n = 1$ is equivalent to $(a)x + (-n)k = 1$.

($\leftarrow$) Given $gcd(a, n) = 1$, It is easy to show $gcd(a, (-1)n) = 1$ as any negative divisor won't ever be the gcd. By *theorem 0.2* there exists x_0 and k_0 such that $(a)x_0 + (-n)k_0 = gcd(a, n) = 1$.

($\rightarrow$) We have x_0 and k_0 which satisfy $(a)(x_0) + (n)(-k_0) = 1$. But 1 is the smallest positive integer satisfying it. It follows $1 = gcd(a, n) = d$.

13

By definition $gcd(m, n) = 1$ and hence we get $m(s_0) + n(t_0) = 1$. Multiplying both sides by r, We get $m(s_0 \cdot r) + n(t_0 \cdot r) = r$.

20

Assume for contradiction that $p_1p_2\dots p_n + 1$ is divisable by p_i. Then

$$\frac{p_1p_2\dots p_n+1}{p_i} = \frac{p_ik_0}{p_i}$$
$$\frac{p_1\dots p_n}{p_i} + \frac{1}{p_i} = k_0$$
$$\frac{p_1\dots p_n}{p_i} - k_0 = \frac{1}{p_i}$$

$L.H.S$ is clearly an integer implying $\frac{1}{p_i}$ is an integer also. Contradiction.

28

$2^n \cdot 3^{2n} = 18^n$. Since $18 \mod 17 = 1$, We get $18^2 \mod 17 = 1 \cdot 1 \mod 17 = 1$. Generally $18^n \mod 17 = 1$, and finally $18^n - 1 \mod 17 = 1 - 1 \mod 17 = 0$.

33

We prove a relaxed version of the problem and hence assume a is positive.

We show the contrapositive. Consider S which does not contain every integer $z \geq a$. Then there's some integer $z_0 \geq a$ where $z_0 \notin S$. In other words the set $R = \{z \mid z \geq a \land z \notin S\}$ is not empty. By the well-ordering principle R has a smallest member, Call it z_s. Note $z_s \neq a$ So we can safely take $z_s - 1 \in S$. Therefore it is NOT the case that if integer $z \in S$ then $z + 1 \in S$ by the counter-example we constructed.

For a general version of any integer a, We would partition set R to a finite subset of non-positives and another subset of positives. Then we consider the smallest of positives by well-ordering, and smallest of non-positives, and take the minimum of both. Recall any finite set has a smallest member.

35

Note $(n+3)^3 = n^3 + 9(n^2 + 3n + 3)$ by trivial algebraic operations.

Base. $n = 1$. $n^3 + (n+1)^3 + (n+2)^3 = 1 + 8 + 27 = 36 = 9(4)$.

Hypo. $n^3 + (n+1)^3 + (n+2)^3 = 9k_0$

Step. $(n+1)^3 + (n+2)^3 + (n+3)^3 = n^3 + (n+1)^3 + (n+2)^3 + 9(n^2+3n+3) = 9k_0 + 9(n^2 + 3n + 3) = 9(k_0 + n^2 + 3n + 3)$

57

2. Let $a_0, a_1 \in A$ where $(\beta\alpha)(a_0) = (\beta\alpha)(a_1)$. In other notation, $\beta(\alpha(a_0)) = \beta(\alpha(a_1))$. Since β is one-to-one we get $\alpha(a_0) = \alpha(a_1)$. Since α is one-to-one we get $a_0 = a_1$.

3. Let $c \in C$. Since β is onto we get $\beta(b_0) = c$. Since α is onto we get $\alpha(a_0) = b_0$. Thus $\beta\alpha(a_0) = c$.

4. For the sake of brevity we highlight that fact the inverse a^{-1} is a well-defined function, i.e maps each element of the domain to exactly one element of the range, as a is both one-to-one and onto.

58

Reflexive. $a - a = 0$.

Symmetry. Given $a - b = z$ is an integer, Trivially $b - a = -z$ is an integer also.

Transitivity. Given $a - b = z_0$ and $b - c = z_1$, Trivially $(a-b)+(b-c) = a - c = z_0 + z_0$ is an integer also.

A Class has numbers of the same decimal fraction.

59

No.

63

$3^{100} \mod 10$ and $2^100 \mod 10$ respectively.