

- (1) (5 points) Let a and b be integers. Show that the value of $\gcd(a^2 + b, 2a^3 + 2ab + 2)$ is either 1 or 2?
[Hint: use the main idea of the Euclidean algorithm, that is, $\gcd(x, y) = \gcd(x, y - zx)$ for any z].

$$\gcd(\underbrace{a^2 + b}_x, \underbrace{2a^3 + 2ab + 2}_y) = \gcd(\underbrace{a^2 + b}_x, \underbrace{2a^3 + 2ab + 2 - 2a(a^2 + b)}_{z-x})$$

$$= \gcd(a^2 + b, 2)$$

Now ~~is a~~ $\gcd(a^2 + b, 2)$ is a positive divisor of 2
hence = 1 or 2

(depending upon whether $a^2 + b$
is even or odd),

- (2) (15 points)

- (a) Find $\gcd(31, 21)$ using the Euclidean algorithm.
(b) Find all positive integer solutions to the equation $31x + 21y = 1770$.
(c) Find all solutions to the congruence $31x \equiv 1770 \pmod{21}$.

$(9, 71), (30, 40), (51, 9)$
are the positive solutions

(a)

$$\underline{31} = \underline{21} + \underline{10}$$

$$\underline{21} = 2 \underline{10} + \underline{1}$$

$$\gcd = 1, \quad \underline{1} = \underline{31} - 2 \underline{10} = \underline{21} - 2(\underline{31} - \underline{21})$$

$$= 3 \underline{21} - 2 \cdot \underline{31}$$

b-contd

Positive integer solution

$$x \geq 0 \Rightarrow 21t \geq 2(1770)$$

$$t \geq \frac{2(1770)}{21}$$

$$y \geq 0 \Rightarrow 31t \leq 3(1770)$$

$$t \leq \frac{3(1770)}{21}$$

$$\Rightarrow t = 16, 17, 171$$

(b)

Solutions exist because $\gcd(31, 21) = 1$

multiply $\underline{1} = (-2)31 + 21(3)$ by 1770

$$\underline{1770} = (-2 \cdot 1770)31 + (3 \cdot 1770)21$$

so one solution is $x_0 = -2(1770)$

$$y_0 = 3 \cdot (1770)$$

all solutions $x = x_0 + 21t \quad t \in \mathbb{Z}$

$$y = y_0 - 31t$$

(c) that there is
We know exactly one
solution modulo 21
(because $\gcd(31, 21) = 1$)
we also know one solution

x_0 from (b)

so
solution is

$$x \equiv -2(1770) \pmod{21}$$

(3) (10 points) Show that the cube of an integer is of the form $7k$, $7k+1$ or $7k+6$.

Cases $a \equiv 0 \pmod{7} \Rightarrow a^3 \equiv 0 \pmod{7} \Rightarrow a^3$ is of the form $7k$

$$a \equiv 1 \pmod{7} \Rightarrow a^3 \equiv 1 \pmod{7} \Rightarrow \text{"} \quad 7k+1$$

$$a \equiv 2 \pmod{7} \Rightarrow a^3 \equiv 8 \pmod{7} \Rightarrow \text{"} \quad 7k+1$$

$$\equiv 1 \pmod{7}$$

$$a \equiv 3 \pmod{7} \Rightarrow a^3 \equiv 27 \pmod{7} \Rightarrow \text{"} \quad 7k+6$$

$$\equiv 6 \pmod{7}$$

$$a \equiv 4 \pmod{7} \Rightarrow a^3 \equiv 64 \pmod{7} \Rightarrow \text{"} \quad 7k+1$$

$$\equiv 1 \pmod{7}$$

$$a \equiv 5 \pmod{7} \Rightarrow a^3 \equiv 5 \cdot 5 \cdot 5 \equiv -8 \pmod{7} \Rightarrow \text{"} \quad 7k+6$$

$$\equiv 6 \pmod{7}$$

$a \equiv 6 \pmod{7}$
 $a^3 \equiv 6 \cdot 6 \cdot 6 \pmod{7}$
 $\equiv (-1)^3 \pmod{7}$
 $\equiv -1 \pmod{7}$
 $\equiv 6 \pmod{7}$
 so a^3 is of the form $7k+6$

(4) (5 points) Show that $2^{32} - 1$ is divisible by 17.

$$2^4 = 16 \equiv -1 \pmod{17}$$

$$\text{so } 2^{32} \equiv (2^4)^8 \equiv (-1)^8 \equiv 1 \pmod{17}$$

$\Rightarrow 2^{32} - 1$ is divisible by 17.

(5) (10 points)

(a) Show that any integer N is congruent modulo 9 to the sum of its digits (in the decimal system).

(b) Given an integer N , let M be the integer obtained by reversing the digits of N . For example if $N = 1325$, then $M = 5231$. Show that $N - M$ is always divisible by 9.

(a) Let $N = a_m \cdot 10^m + \dots + a_0$

$$10 \equiv 1 \pmod{9} \text{ so}$$

$$N \equiv a_m + \dots + a_0 = \sum a_i \pmod{9}$$

(b) $N \equiv \sum a_i \pmod{9}$

and $M \equiv \sum a_i \pmod{9}$

$$\sum a_i$$

digits of M are the same (but in reverse order) as that of N .
 $\Rightarrow N \equiv M \pmod{9} \Rightarrow 9 | M - N$

(6) (5 points) Prove that $\sqrt{11}$ is an irrational number.

Suppose not $\sqrt{11} = \frac{a}{b}$

assume (by cancelling common factors) that $\gcd(a, b) = 1$

Therefore $11 = \frac{a^2}{b^2}$ or $a^2 = 11b^2$

Case 1: If $b = 1$, then $a^2 = 11$ but 11 is not a square of any integer

$[n^2 > 11 \text{ if } n > 3$

$1^2 \neq 11$

$2^2 \neq 11$

$3^2 \neq 11$

]

Therefore this cannot happen

Therefore only possibility is

Case 2 ~~if~~ $b \neq 1$: ~~then~~ pick a prime number p dividing b .

$\Rightarrow p | 11b^2 \Rightarrow p | a^2 \Rightarrow p | a$ so p divides both a and b

$\Rightarrow p$ is a common factor of a, b

$\Rightarrow \gcd(a, b) = 1 \Rightarrow \Leftarrow$