Sample: Discrete Mathematics - Congruence and Forms of a Number

Question 1. Consider the sequence: 0, 3, 8, 15, 24, 35, 48, ...

a) Find an explicit formula which generates the sequence (Hint: Think perfect squares).

Solution.

If we take $a_n = n^2$, then we get the sequence 1, 4, 9, 16, 25, 36, 49 … . So, it easily seen, if we subtract 1, we get the sequence 0, 3, 8, 15, 24, 35, 48, … . Hence, the explicit formula for required sequence is $b_n = n^2 - 1$.

Answer: $b_n = n^2 - 1$.

b) Find a recursive formula, which generates the sequence (Hint: Think successive differences).

Solution.

Consider n +1- th term of the sequence $b_{n+1} = (n+1)^2 - 1 = n^2 + 2n + 1 - 1 = (n^2 - 1) + 2n + 1 = b_n + 2n + 1$. So, a recursive formula which generates the sequence is $b_{n+1} = b_n + 2n + 1$.

Answer: $b_{n+1} = b_n + 2n + 1$.

Question 2. Matrix Multiplication.

a) Find a pair of 2x2 matrices satisfying: A· B ≠ B· A.

Solution.

Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. Then $A * B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $B * A = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. Obviously, A· B ≠ B· A.

Answer: $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$.

b) Find a pair of 2 × 2 matrices satisfying: A·B = 0, with both A≠ 0 and B ≠ 0.

Solution.

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, and B is arbitrary matrix $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Let find a,b,c,d such that $A * B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. $A * B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$. Hence, a=0,b=0 and c and d are arbitrary numbers except zeroes. So, for example, we can take $B = \begin{pmatrix} 0 & 0 \\ 4 & 1658 \end{pmatrix}$.

Answer: $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 4 & 1658 \end{pmatrix}$.

Question 3. Number systems:

a) Find the binary, octal and hexadecimal expansions of 1292_{10}.

Answer:

Binary expansions

The integer part of dividing	Modulo
1292 div 2 = 646	1292 mod 2 = 0
646 div 2 = 323	646 mod 2 = 0
323 div 2 = 161	323 mod 2 = 1
161 div 2 = 80	161 mod 2 = 1

80 div 2 = 40	80 mod 2 = 0
40 div 2 = 20	40 mod 2 = 0
20 div 2 = 10	20 mod 2 = 0
10 div 2 = 5	10 mod 2 = 0
5 div 2 = 2	5 mod 2 = 1
2 div 2 = 1	2 mod 2 = 0
1 div 2 = 0	1 mod 2 = 1

So, the binary expansion (we should add the modulus from the bottom to the top) is $10100001100_2 = 1292_{10}$.

Answer:$10100001100_2 = 1292_{10}$.

Octal expansion

The integer part of dividing	Modulo
1292 div 8 = 161	1292 mod 8 = 4
161 div 8 = 20	161 mod 8 = 1
20 div 8 = 2	20 mod 8 = 4
2 div 8 = 0	2 mod 8 = 2
0 div 8 = 0	0 mod 8 = 0

So, as in previous case after adding modulus we get $2414_8 = 1292_{10}$.

Answer:$2414_8 = 1292_{10}$.

Hexadecimal expansion

The integer part of dividing	Modulo
1292 div 16 = 80	1292 mod 16 = 12
80 div 16 = 5	80 mod 16 = 0
5 div 16 = 0	5 mod 16 = 5
0 div 16 = 0	0 mod 16 = 0

So, as in previous cases after adding modulus we get $50C_{16} = 1292_{10}$ (because in Hexadecimal expansion $12_{10} = C_{16}$).

Answer: $50C_{16} = 1292_{10}$.

b) Find the octal, decimal and hexadecimal expansions of11101110110111_2

Decimal form. To convert, we need to multiply the number digit by it's corresponding power of discharge

11101110110111_2 = 2^{13}*1 + 2^{12}*1 + 2^{11}*1 + 2^{10}*0 + 2^9*1 + 2^8*1 + 2^7*1 + 2^6*0 + 2^5*1 + 2^4*1 + 2^3*0 + 2^2*1 + 2^1*1 + 2^0*1 = 8192 + 4096 + 2048 + 0 + 512 + 256 + 128 + 0 + 32 + 16 + 0 + 4 + 2 + 1 = 15287.

Answer: $11101110110111_2 = 15287_{10}$.

Octal form. We group the source code into groups of 3 digits. $11101110110111_2 = 011\ 101\ 110\ 110\ 111\ _2$.

Then replace each group with the code from the table.

Binary	Octal
000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

Hence, we get a number: $011\ 101\ 110\ 110\ 111\ _2 = 35667_8$

Answer: $11101110110111_2 = 35667_8$.

Hexadecimal form

We group the source code into groups of 4 digits.

$11101110110111_2 = 0011\ 1011\ 1011\ 0111\ _2$.

Then replace each group with the code from the table.

Binary	Hexadecimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Hence, we get a number: $0011\ 1011\ 1011\ 0111_2 = 3BB7_{16}$.
Answer: $0011\ 1011\ 1011\ 0111_2 = 3BB7_{16}$.

Question 4. Primes:

a) Which of 5293 and 8191 is prime?
Solution.
To verify is the number prime or not we should examine if this number can be divided to all primes less or equal than integer part of its root. So, the integer part of the square root from 5293 is 72. And all primes less than 72 are 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71. It is easy to check that 5293 is divisible by 67. Similarly, we can check that 8191 is prime.
Answer.5293 is not prime; 8191 is prime.

b) Factor the one which is not a prime.
Answer. 5293=67*79

c) Is the prime a Mersenne prime?
Solution.
In mathematics, a Mersenne prime is a prime number of the form $M_n = 2^n - 1$, where n is a prime number.
8191 is a Mersenne prime, because 8191+1=8192 and $8192 = 2^{13}$.

Question 5. Modular Arithmetic. Compute:

a) (724 mod (11) + 843 mod (11)) mod (11).
b) (724+843) mod (11).
c) (724 mod (11) · 843 mod (11)) mod (11).
d) (724· 843) mod (11).
e) $2141^{2141}\ mod\ (11)$. (Hint: Fermat's Little Theorem).

Solution.

a) (724 mod (11) + 843 mod (11)) mod (11) ≡ (9 +7)mod(11) ≡ 16 mod (11)=5.
b) (724+843) mod (11) ≡ 1567 mod(11) ≡ 5.
c) (724 mod (11) · 843 mod (11)) mod (11) ≡ (9·7) mod (11) ≡ 63 mod (11)=8.
d) (724· 843) mod (11) ≡ 9· 7 mod (11) ≡ 8.
e) Using Fermat's Little Theorem we get $2141^{10} \equiv$ 1 mod (11). So, 2141^{10}mod (11) ≡ 1. Since

If a ≡ b mod (p), then $a^n \equiv b^n mod(p)$, we get $2141^{2141} mod(11) \equiv$
$2141^{2140} * 2141$mod(11) ≡ $(2141^{10})^{214} * 7\ mod\ (11) \equiv 1 * 7\ mod\ (11) \equiv 7$.

Question 6. Using one of the "definitions" that:

a ≡ b mod(p) means p | (a-b), or,
a ≡ b mod(p) means ∃k (a — b = kp), or,
a ≡ b mod(p) means a/b&b/p have same remainder;
prove each of the following:

a) If a ≡ b mod p and c ≡ d mod p, then a+c ≡ b+d modp.

b) If a $\equiv$ b modp and c $\equiv$ d modp, then ac $\equiv$ bd modp.
c) If a $\equiv$ b modp, then $a^c \equiv b^c$ modp.

Solution.

We will use second definition a $\equiv$ b mod(p) means ∃k (a — b = kp).

a) ∃k (a — b = kp), ∃n (c — d = np), lets add this, so a-b+c-d =kp+np, (a+c) –(b+d)=(k+n)p. Hence, we get for a+c and b+d exists k+n such that (a+c) –(b+d)=(k+n)p. Thus, a+c$\equiv$b+d modp.

b) By definition ∃k (a — b = kp), ∃n (c — d = np). That is a=b+kp, c= d+np, after multiplaing this equations, we get ac=bd+bnp+kdp+kpnp=bd +(bn+kd+kpn)·p. Hence, we get a number bn+kd+kpn such that ac= bd + (bn+kd+kpn)·p, that is ac$\equiv$bd mod (p).

c) c is integer >0. Take c=2. $\exists k\ (a-b=kp)$; $a=b+kp$. Multiply a*a: $a*a=a^2=(b+kp)(b+kp)=b^2+2bkp+k^2p^2 \to a^2-b^2=(2bk+k^2p)*p$. Hence, we can get a number $2bk+k^2p$ such that $a^2=b^2\ mod(p)$. If $c=n\in Z_+$:

$$a*a*\ldots*a=a^n=(b+kp)*\ldots*(b+kp)=(b+kp)^n=b^n+q*p,$$

where q is integer positive number. So, we obtain that $a^n-b^n=q*p\to a^n=b^n\ mod(p)$.

Question 7. Find a & b, with a = b mod(11) ≠ 0, satisfying:

$$(3^a)mod(11) \neq (3^b)mod(11).$$

Solution.

Let's take a=1, b=12, it is easily seen that a$\equiv$ b mod (11). $3^{12}mod\ (11)=3^{10}*3^2\ mod\ (11)$. Similarly, as in the previous question using Fermat's Little Theorem ($if\ p-prime$, a is not divisible by p $then$ $a^{p-1}=1\ mod\ p$. In this case a=3, p =11, so $3^{10}=1\ mod\ (11)$) we get $3^{12}mod\ (11)=3^{10}3^2*mod\ (11)=9\ mod\ (11)\neq 3\ mod\ (11)$.

Question 8. Solve: 8x + 7 = 5 mod (11)

Solution.

Let's solve this through trial. Consider a complete system of residues modulo 11: (0,1,2,3,4,5,6,7,8,9,10). And residue 8 satisfies the congruence.

Answer. $x=8\ mod\ 11$.