1:

Number Theory covers many of the most important topics in mathematics and they are all very deeply and intrinsically connected together.

Starting with divisibility, we say that a nonzero b divides a if a = mb for some m, where a, b and m are integers. A common notation for this is b|a, therefore we say b|a we say that b is divisor of a. a few properties of divisibility are a|1, then a += 1, if a|b and b|a then a+= b.

Euclidean algorithm is one of the basic techniques of number theory. It is a procedure for determining the greatest common divisor of two positive integers. Two integers are relatively prime if their only common positive integer factor is 1. The greatest common divisor of a and b is the largest integer that divides both a and b. We can use the notation gcd(a,b) to mean the greatest common divisor of a and b therefore we also define gcd(0,0)=0. Euclidian algorithm is for easily finding the greatest common divisor of two integers.

Modular arithematic, if an there is an integer a and n is another positive integer, we define a mod n t be the remainder when a is divided by n, then the integer is called the modulus.

A = qn + r 0<= r <n; q=[a/n]

Two integers a and b are then said to be congruent modulo n if (a mod n) =(b mod n).

This is written as a = b(mod n). there are properties of congruence such as a=n(mod n) if n|(a-b), a=b(mod n) implies b = a(mod n), a=b(mod n) and b=c(mod n) imply a=c(mod n).

Prime numbers only have divisors of 1 and itself, and they cannot be written as a product of other numbers, they are very central to number theory. Any integer a>1 can be factored ina unique way. This is knonw as the fundamental theorem of arithmetic.

Fermat’s little theorem states the following, that is p is a prime and a is a positive integer not divisible by p then a^p-1 = 1(mod p),

An alternate form of this is a^p = a(mod p). this is veery important in public-key cryptography.

2:

N = pq= 77, then p and q equal 7 and 11

ø(n) = (p-1)(q-1)

ø(n) = (6)(10)

ø(n) = 60

d\*13 = 1 mod 60 and d < 60

for d in range(60):

if (d \* 13) % 60 == 1:

print(d)

d must be 37

M = C^d mod n

M = 20^37 mod 77

M = 48

3:

Calendar

Description automatically generated

6472 mod 3415 = 3346

4:

A)

Table

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
| 5C | 6B | 05 | F4 |
| 7B | 72 | A2 | 6D |
| B4 | 34 | 31 | 12 |
| 9A | 9B | 7F | 94 |

|  |  |  |  |
| --- | --- | --- | --- |
| 4A | 7F | 6B | BF |
| 21 | 40 | 3A | 3C |
| 8D | 18 | C7 | C9 |
| B8 | 14 | D2 | 22 |

B) Diagram

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
| 67 | A7 | 78 | 97 |
| 99 | A6 | D9 | 35 |
| 68 | 0F | 61 | 68 |
| FA | B1 | 21 | 82 |

|  |  |  |  |
| --- | --- | --- | --- |
| 67 | A7 | 78 | 97 |
| 35 | 99 | A6 | D9 |
| 61 | 68 | 68 | 0F |
| B1 | 21 | 82 | FA |