Number Theory

Examples

Steven Gordon

1 Modular Arithmetic

The following examples are using modulus of 10.

1.1 Calculating the remainder

3 mod 10 = 3	since 0 x 10 + 3 = 3
13 mod 10 = 3	since 1 x 10 + 3 = 13
-7 mod 10 = 3	since -1 x 10 + 3 = -7

$3 \equiv 13 \equiv -7 \pmod{10}$

1.2 Addition

4 + 3 = 7
4 + 7 = 11 = 1
4 + 13 = 4 + 3 = 7

1.3 Additive Inverse

$A + B \equiv C \pmod{n}$

B is an additive inverse of A if C = 0

1 is an additive inverse of 9 since $1 + 9 \equiv 0 \pmod{10}$

6 is an additive inverse of 4

Also, $-1 \equiv 9 \pmod{10}$ and $-4 \equiv 6 \pmod{10}$

1.4 Subtraction

4 – 7 = 4 + (-7) = 4 + 3 = 7
8 – 9 = 8 + (-9) = 8 + 1 = 9

1.5 Multiplication

4 x 7 = 28 mod 10 = 8
9 x 12 = 108 mod 10 = 8

1.6 Multiplicative Inverse

$A \times B \equiv C \pmod{n}$
B is a multiplicative inverse of A if C = 1
1 is its own multiplicative inverse: 1 x 1 = 1 (mod 10)
3 is the multiplicative inverse of 7: 3 x 7 = 1 (mod 10)
9 is its own multiplicative inverse: 9 x 9 = 1 (mod 10)

2 Prime Numbers

The divisors of 3 are 1 and 3 (itself), therefore prime.
The divisors of 4 are 1, 4 (itself) and 2, and therefore not prime (composite).

2.1 Greatest common divisor

The gcd of 24 and 18 is 6.

The gcd of two prime numbers is 1. E.g. gcd (19,17) = 1

Gcd (24,-18) = 6

3 Fermat's Theorem

$p = 5$, $a = 3$
$a \pmod p \equiv 3$

$a^p = 3^5 = 243$
$243 \equiv 3 \pmod 5 = a \pmod p$
Or 243 mod 5 = 3

$p = 5$, $a = 11$
$a \pmod p \equiv 1$

$a^p = 11^5 = 161051$
$161501 \equiv 1 \pmod 5 = a \pmod p$

4 Eulers Totient Function

$\varnothing(37)$
Since 37 is prime, $\varnothing(37) = 36$

$\varnothing(35)$
All integers less than 35 that are relatively prime to 35:
1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17 18, 19 22, 23, 24, 26, 27, 29, 31, 32, 33, 34
(why? What can divide 35? 1, 5, 7 and 35. So all numbers less than 34 that can also be divided by 5 and 7 are not relatively prime, e.g. 5, 7, 10, 14, 15, 20, 21, …)
24 integers so $\varnothing(35) = 24$

5 Euler's Theorem

$a = 3$; $n = 10$; $\varnothing(10) = 4$

$a^{\varnothing(n)} = 3^4 = 81$
81 mod 10 = 1 or $81 \equiv 1 \pmod n$

$a = 2$; $n = 11$, $\varnothing(11) = 10$
$a^{\varnothing(n)} = 2^{10} = 1024$
1024 mod 11 = 1
$1024 \equiv 1 \pmod{11} = 1 \pmod n$