CSS322 – Number Theory Summary

Modular Arithmetic

Addition: $a+b(mod\ n)\equiv(a+b)mod\ (n)$
Additive Inverse: if $a+b(mod\ n)\equiv 0$ then *a* is additive inverse of *b*, or $a=AI(b)$
Every number has a additive inverse.
Subtraction: $a-b(mod\ n)\equiv a+AI(b)(mod\ n)$
Multiplication: $a*b(mod\ n)\equiv(a*b)mod\ (n)$
Multiplicative Inverse: if $a*b(mod\ n)\equiv 1$ then *a* is amultiplicative inverse of *b*, or $a=MI(b)$
Not every number has a multiplicative inverse. In fact, a number *a* has a multiplicative inverse in (*mod n*) if *a* and *n* are relatively prime or $gcd(a,n)=1$
Division: $a/b(mod\ n)\equiv a*MI(b)(mod\ n)$
Exponentiation: $a^b(mod\ n)\equiv(a^b)mod\ n$
Property of multiplication: $(a*b)(mod\ n)\equiv[(a\ mod\ n)*(b\ mod\ n)]mod\ (n)$
Inverse Exponentiation is called **Discrete Logarithm**: $dlog_{a,n}(b)$ is x such that $b\equiv a^x(mod\ n)$
Not every number has a discrete logarithm. Calculating the discrete logarithm of very large numbers if very difficult.

Prime Numbers

A **prime number**, *p*, is an integer if $p>1$ and if and only if the only divisors of *p* are ±1 and ±*p*.
Any integer, $a>1$ can be factored by only prime numbers.
Determining the prime factors of a very large integer is very difficult.
Relatively Prime: Two integers *a* and *b* are relatively prime if they have no prime factors in common. Or in other words, if $gcd(a,b)=1$ then *a* and *b* are relatively prime.
The integer 1 is relatively prime with every other integer.

Fermat's and Euler's Theorems

Fermat's Theorem: if *p* is prime and *a* is a positive integer not divisible by *p*, then:

$$a^{p-1}\equiv 1(mod\ p)$$

Or alternatively, if *p* is prime and *a* is a positive integer:

$$a^p\equiv a(mod\ p)$$

Euler's Totient: $\phi(n)=x$ where *x* is the count of integers less than *n* that are relatively prime with *n*.
If *p* is prime, $\phi(p)=p-1$.
If *p* and *q* are prime, $\phi(p*q)=\phi(p)*\phi(q)=(p-1)*(q-1)$

Euler's Theorem: For every *a* and *n* that are relatively prime:

$$a^{\phi(n)}\equiv 1(mod\ n)$$

Or alternatively, for any integers *a* and *n*:

$$a^{\phi(n)+1}\equiv a(mod\ n)$$