NU1 Statements

A Collection of Unsubstantiated Claims

Nick Spinale

Budapest Semesters in Mathematics

Number Theory

December 1, 2016

Divisibility

Notation. $a|b \iff \exists x : ax = b$

Proposition.

1. $a|b \implies a|bc$
2. $a|b$ and $b|c \implies a|c$
3. $a|b$ and $a|c \implies a|bx + cy$
4. $a|b$ and $b \neq 0 \implies |a| \leq |b|$
5. $a|b$ and $b|a \implies a = \pm b$

Proposition. $a^n - b^n = (a - b) \sum_{i=0}^{n-1} a^{n-i} b^i$

Proposition. If n is odd, then $a^n + b^n = (a + b) \sum_{i=0}^{n-1} (-1)^i a^{n-i} b^i$

Proposition. If n is composite, then $2^n - 1$ is also composite.

Proposition. If $n \geq 2$ and $a^n - 1$ is prime, then $a = 2$ and n is prime.

Definition (Fermat numbers)**.** $F_n = 2^{(2^n)} + 1$

Proposition. $(F_n, F_m) = 1$

Definition. d, denoted (a, b), is the distingiushed common divisor of a and b iff

1. $d|a$ and $d|b$
2. $c|a$ and $c|b \implies c|d$

Proposition. (a, b) exists, and is unique up to sign.

Definition (Euclidean Algorithm)**.** Todo

Proposition.

1. $(a, b) = (a, ak + b)$
2. $(ma, mb) = m(a, b)$

Definition (Euclidean Algorithm)**.** (a, b) is the smallest n such that $ax + by = n$.

Definition. a and b are relatively prime iff $(a, b) = 1$.

Lemma (Euclid)**.** $a|bc$ and $(a, b) = 1 \implies a|c$

Base 10 Divisibility

Proposition (Divisibility by 9)**.** $\overline{a_k \dots a_1 a_0} \equiv a_k + \dots + a_1 + a_0 \mod 9$

Proposition (Divisibility by 11)**.** $\overline{a_k \dots a_1 a_0} \equiv \sum_{i=0}^{k} (-1)^n a_i \mod 11$

Proposition (Last k digit rule)**.** If $n | 10^k$, then $\overline{\dots a_k a_{k-1} \dots a_1 a_0} \equiv \overline{a_{k-1} \dots a_2 a_1} \mod n$

Primes

Definition. p is irreducable iff $a|p \implies a = 1 \vee a = p$

Definition. p is prime iff $p|ab \implies p|a \vee p|b$

Proposition. In $\mathbb{Z}$, irreducability and primality are equivalent.

Theorem (Fundimental Theorem of Arithmetic)**.** Every positive integer n has a unique canonical representation

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

Where $p_1 < p_2 < \dots < p_k$ are primes.

Theorem (Bertrand's Postulate)**.** For all n, there exists a prime p such that $n < p < n2$.

Theorem. Arbitrarily large prime gaps exist.

Theorem (Dirichet)**.** If $(a, b) = 1$, then there are infinitely many primes of the form $ak + b$.

Theorem. $(\exists x : x^2 \equiv -1 \mod p) \iff p = 4k + 1$

Theorem. If $p = 4k - 1$ and $p | a^2 + b^2$, then $p|a$, $p|b$, and $p^2 | a^2 + b^2$.

Congruences

Proposition. Assume $a \equiv b \mod m$ and $c \equiv d \mod m$.

1. $a + c \equiv b + d$
2. $ac \equiv bc$
3. $ac \equiv bd$
4. $a^n \equiv b^n$

Definition.

1. A complete residue system modulo n is a set containing exactly one element from each residue class modulo n.
2. A reduced residue system modulo n is a set containing exactly one element from each residue class modulo n coprime to m.

Definition (Totient function)**.** $\phi(n)$ is the number of integers a such that $1 \leq a < n$ such that $(a, n) = 1$.

Proposition. Assume $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Then $\phi(n) = \prod (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod (1 - \frac{1}{p_i})$

Theorem (Euler's totient theorem)**.** If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.

Theorem (Wilson)**.** $(p - 1)! \equiv -1 \mod p$

Theorem. The congruence $ax \equiv b \mod m$ has a solution iff $(m, a) | b$. Furthermore, all such solutions are equivalent modulo $\frac{m}{(m,a)}$.

Corollary. $ab \equiv ac \mod m \iff b \equiv c \mod \frac{m}{(m,a)}$

Corollary. The equation $ax + by = c$ has a solution iff $(a, b) | c$. Furthermore, if (x_0, y_0) is a solution, then so is $(x_0 - t\frac{b}{(a,b)}, y_0 + t\frac{a}{(a,b)})$.

Theorem (Chinese Remainder Theorem)**.** If $n_1, \dots n_k$ are pairwise coprime and $\Pi n_i = N$, then $x \mod N \mapsto (x \mod n_1, \dots x \mod n_k)$ is a ring isomorphism.

Interesting Numbers

Theorem. If m and n are each the sum of two squares, then so is mn.

Theorem. n is the sum of two squares iff $n = 2^\gamma \prod p_i^{\alpha_i} \prod q_i^{2\beta_i}$, where $p_i = 4k+1$ and $q_i = 4k-1$.

Order

Definition (Order)**.** Given modulus n and g such that $(n, a) = 1$, the order of g is the smallest positive k such that $g^k \equiv 1(n)$. We say $o_n(g) = k$.

Proposition. $o_n(g)|\phi(n)$

Proposition. $o_n(g^i) = \frac{o_n(g)}{(i, o_n(g))}$

Definition (Primitive Root)**.** g is a primitive root modulo n if $o_n(g) = \phi(n)$.

Theorem. There exists a primitive root modulo n iff one of the following is true:

$$\begin{aligned}
&n = p^\alpha \text{ for some odd prime } p\\
&n = 2p^\alpha \text{ for some odd prime } p\\
&n = 2\\
&n = 4
\end{aligned}$$

Theorem. $\sum_{d|n} \phi(n) = n$

Quadratic Residues