Elements of Number Theory

Ben Church

Contents

1 The Integers and Divisibility

Number Theory is primarily the study of the integers $\mathbb{Z}$. In this course we will study specific subsets and supersets of the integers.

1.1 Basic Definitions

Definitions of Common Sets:

- $\mathbb{Z}^+ \ = \{n \in \mathbb{Z} \mid n > 0\}$
- $\mathbb{P} \ = \{p \in \mathbb{Z}^+ \mid p \text{ is prime}\}$
- $\mathbb{N} \ = \{n \in \mathbb{Z} \mid n \geq 0\}$
- $\mathbb{Q} \ = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \ \wedge \ n \neq 0\}$

Fact: $\mathbb{P} \subset \mathbb{Z}^+ \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

Definition: Let $n, a \in \mathbb{Z}$ then $n \mid a \iff \exists x \in \mathbb{Z} : nx = a$

Definition: $p \in \mathbb{Z}^+$ and $p > 1$ is prime iff $\forall a \in \mathbb{Z}^+(a \mid p \implies a = 1 \vee a = p)$
equivalently: if $a, b \in \mathbb{Z}^+$ s.t. $p = ab$ then $a = 1$ or $b = 1$

Definition: Let $n, a, b \in \mathbb{Z}$ then $a \equiv b \bmod n \iff n \mid a - b$

1.2 Well-Ordering and Induction

The natural numbers have two particularly important properties known as the well-ordering principle and the principle of mathematical induction. These two properties are logically equivalent (see Theorem 1.1) but neither can be proved from other elementary properties. One of these two statements is conventionally included as an axiom of the natural numbers.

The Well-Ordering Principle:
If $A \subseteq \mathbb{N} \wedge A \neq \{\}$ then $\exists x \in A : \forall y \in A : x \leq y$.
I.e. every non-empty subset of $\mathbb{N}$ has a least element.

The Principle of Mathematical Induction:
If ϕ is a logical predicate which satisfies:

1. $\exists g \in \mathbb{N} : \phi(g)$
2. $\forall x \in \mathbb{N} : \phi(x) \implies \phi(x+1)$

   then $\forall x \in \mathbb{N} : x \geq g \implies \phi(x)$

Theorem 1.1. *well-ordering is equivalent to induction*

Proof. Suppose well-ordering. Let ϕ satisfy the induction criteria.
Define:

$$S = \{n \in \mathbb{N} \mid \neg\phi(n) \ \wedge \ n \geq g\}$$

Assume $S \subseteq \mathbb{N}$ is not empty. By well-ordering, S has a least element l.
$l - 1 < l$ so $l - 1 \notin S$. Also, $l > g$ because $\phi(g)$ and therefore, $l - 1 \geq g$.
But $l - 1 \notin S$ thus, $\phi(l-1)$ so by criterion 2, $\phi(l)$ thus $l \notin S$. $\boxtimes$ (a contradiction!)
Therefore, $S = \{\}$ so $\forall x \in \mathbb{N} : \neg(\neg\phi(n) \ \wedge \ n \geq g)$ i.e. $n \geq g \implies \phi(x)$

Suppose induction. Let $A \subseteq \mathbb{N}$ have no least element.
Define:

$$\phi(n) \iff \forall x \leq n : x \notin A$$

Since 0 is the least element of all the natural numbers, $0 \notin A$ thus $\phi(0)$
Suppose $\phi(n)$, if $n + 1 \in A$ then because $\forall x < n + 1 : x \notin A$
$n + 1$ would be the least element of A but A does not have a least element. $\boxtimes$
Thus, $n + 1 \notin A$ so $\forall x \leq n + 1 : x \notin A$ which implies $\phi(n + 1)$
By induction, $\forall x \in \mathbb{N} : \phi(n)$ so $\forall n \in \mathbb{N} : n \notin A$ equivalently $A \cap \mathbb{N} = \{\}$
note that $A \subseteq \mathbb{N}$. Thus: $A = \{\}$

Induction proves that if A has no least element then A is empty.
Equivalently, if A is not empty then A has a least element.

$\square$

1.3 Properties of Modular Arithmetic

Lemma 1.2. *If $n \mid a$ and $n \mid b$ then $\forall x, y \in \mathbb{Z} : n \mid ax + by$*

Proof. Let $a = ns$ and $b = nr$ then $ax + by = n(sx + ry)$.
Because $sx + ry \in \mathbb{Z}$ we conclude that $n \mid ax + by$

Lemma 1.3. *If $an \mid bn$ then $a \mid b$*

Proof. Let $ank = bn$ therefore, $ak = b$ so $a \mid b$

Lemma 1.4. *modular congruence is what is known as an equivalence relation*

1. *(Reflexivity) For every $a \in \mathbb{Z}$, $a \equiv a \bmod n$*
2. *(Symmetry) If $a \equiv b \bmod n$ then $b \equiv a \bmod n$*
3. *(Transitivity) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$*

Proof. $a - a = 0$ but $n0 = 0$ so $\exists x$ (namely 0) $: nx = a - a$ therefore, $n \mid a - a$.
If $n \mid a - b$ then $nk = a - b$ so $n(-k) = b - a$ thus $n \mid b - a$.
If $n \mid a - b$ and $n \mid b - c$ then $n \mid (a - b) + (b - c)$ so $n \mid a - c$.

Lemma 1.5. *If* $a \equiv b \bmod n$ *and* $c \equiv d \bmod n$ *then* $a + c \equiv b + d \bmod n$

Proof. $n \mid a - b$ and $n \mid c - d$ thus, $n \mid (a - b) + (c - d)$ so $n \mid (a + c) - (b + d)$

Lemma 1.6. *If* $a \equiv b \bmod n$ *and* $c \equiv d \bmod n$ *then* $ac \equiv bd \bmod n$

Proof. Let $n \mid a - b$ and $n \mid c - d$ then $n \mid (a - b)c + (c - d)b$ thus $n \mid ac - bd$

Lemma 1.7. *If* $a \equiv b \bmod n$ *then* $\forall k \geq 0 :$ $a^k \equiv b^k \bmod n$

Proof. Base Case: by hypothesis $a^1 \equiv b^1 \; mod \, n$
Assume that $a^k \equiv b^k \bmod n$ then by Lemma 1.6, $a^k \cdot a \equiv b^k \cdot b \bmod n$
thus $a^{k+1} \equiv b^{k+1} \bmod n$ and by induction, the result holds for all k.
note: $a^k \equiv b^k \bmod n \quad \not\Rightarrow \quad a \equiv b \bmod n$

1.4 Primes and Factorization

Theorem 1.8. *every* $1 < x \in \mathbb{N}$ *is either prime or a product of primes*

Proof. Let S be the set of natural numbers that are neither prime nor a product of primes. Suppose S is non-empty. By well-ordering, S has a least element: g.
g is not prime so $g = ab$ where $1 < a, b < g$ and since g is minimal, $a, b \notin S$.
Therefore, a and b are either prime or products of primes.
Because products of products of primes are products of primes,
$ab = g$ is a product of primes so $g \notin S$ ⊠

Thus, S is empty.

□

Theorem 1.9. *There are infinitely many primes.*

Proof. Suppose that $p_1, p_2, \ldots, p_k$ are all the primes.
Then we can define: $\Pi = p_1 p_2 \ldots p_k + 1$.
By Theorem 1.8, $\exists \tilde{p} \in \mathbb{P}$ s.t. $\tilde{p} \mid \Pi$
Because $\tilde{p}$ is prime, it must be one of the p_i so $\tilde{p} \mid p_1 p_2 \ldots p_k$.
Thus, $\tilde{p} \mid \Pi - p_1 p_2 \ldots p_k$ therefore $\tilde{p} \mid 1$ ⊠ □

Theorem 1.10 (The Fundamental Theorem of Arithmetic)**.** *Every natural number has a unique prime factorization.*

Proof. Let s be the least natural number with non-unique prime factorization so that $s = p_1 p_2 \ldots p_n$ and that $s = q_1 q_2 \ldots q_m$ where p_1 is not any q_i
Consider $t = (q_1 - p_1) q_2 \ldots q_m = q_1 q_2 \ldots q_m - p_1 q_2 \ldots q_m$
Therefore, $t = s - p_1 (q_2 \ldots q_m)$ but $p_1 \mid s$ so $p_1 \mid t$.
$t < s$ so $t = (q_1 - p_1)(q_2 \ldots q_m)$ has unique factorization.
Because $p_1 \mid t$ and p_1 is not any q_i then $p_1 \mid q_1 - p_1$.
Since $p_1 \mid p_1$ by Lemma 1.3, $p_1 \mid q_1$ but $p_1 \neq q_1$ so q_1 is not prime. ⊠
By well-ordering, every natural number must have a unique prime factorization. □

1.5 The Euclidean Property and Modular Residues

Theorem 1.11 (The Euclidean Property)**.** *Let $a, b \in \mathbb{N}$ then there exist unique $q, r \in \mathbb{N}$ s.t. $a = qb + r$ and $0 \leq r < b$*

Proof. Define:
$$S = \{x \in \mathbb{N} \mid \exists q \in \mathbb{Z} : x = a - bq\}$$

Because $a \in S$, S is non-empty so by well-ordering, S has a least element r.
Since $r \in S$ we know that $r \geq 0$ and for some q, $a = bq + r$.
Suppose that $r > b$ then, $a - bq > a - bq - b = a - b(q+1) > 0$
so $r - b \in S$ but is less than r, the least element. ⊠ □

Lemma 1.12. *Let $a = nq_a + r_a$ and $b = nq_b + r_n$ s.t. $0 \leq r_a, r_b < n$ then $a \equiv b \bmod n \iff r_a = r_b$*

Proof. Let $n \mid a - b$ then $n \mid r_a - r_b + n(q_a - q_b)$ so $n \mid r_a - r_b$.
However, $r_a - r_b < n$ so $r_a - r_b = 0$. Thus $r_a = r_b$.

If $r_a = r_b$ then $a - b = n(q_a - q_b)$ so $n \mid a - b$ i.e. $a \equiv b \bmod n$.

Definition: Let $a = qn + r$ s.t. $0 \leq r < n$, then r is the residue of a modulo n i.e. $a\,mod\,n = r$. By the above, $a\,mod\,n = b\,mod\,n \iff a \equiv b \bmod n$.

Lemma 1.13. *The facts of modular arithmetic can be applied directly to the modular residues which are the most reduced form of that number:*

- $((a\,mod\,n) + (b\,mod\,n))\,mod\,n = (a+b)\,mod\,n$
- $((a\,mod\,n)(b\,mod\,n))\,mod\,n = (ab)\,mod\,n$
- $(a\,mod\,n)^k\,mod\,n = a^k\,mod\,n.$

Proof. The statements rely on: $(a\,mod\,n) \equiv a \bmod n$ and $(b\,mod\,n) \equiv b \bmod n$ by Lemma 1.5 we have that $(a\,mod\,n) + (a\,mod\,n) \equiv a + b \bmod n$ and therefore, $((a\,mod\,n) + (b\,mod\,n))\,mod\,n = (a+b)\,mod\,n$. The other results can be proved in an identical manner.

1.6 Examples of Congruence Calculations

Show: $13 \mid 3^{45} - 1$. $3^{45} = 27^{15}$ and $27 \equiv 1 \bmod 13$ so $27^{15} \equiv 1^{15} \bmod 13$
thus, $3^{45} \equiv 1 \bmod 13$ i.e $13 \mid 3^{45} - 1$

Show: $31 \mid 2^{45} - 1$. $2^{45} = 32^9$ and $32 \equiv 1 \bmod 31$ so $2^{45} \equiv 1^9 \bmod 31$

Show: $13 \mid 2^{24} - 1$. $2^{24} = 16^6$ and $16 \equiv 3 \bmod 13$ so $2^{24} \equiv 3^6 \bmod n$
however, $3^6 = 27^2$ and $27 \equiv 1 \bmod 13$ so $2^{24} \equiv 1 \bmod 13$

Show: $13 \mid 7^{24} - 1$. $7^{24} = 49^{12}$ and $49 \equiv -3 \bmod 13$
so $49^{12} \equiv (-3)^{12} \bmod 13$ however, $(-3)^{12} = 81^4$ and $81 \equiv 3 \bmod 13$.
Thus, $81^3 \equiv 3^3 \equiv 27 \equiv 1\, mod\, 13$ so $7^{24} \equiv 1 \bmod 13$.

Show: $28 \mid 3^{92} - 9$. $92 = 3 \cdot 30 + 2$ and $3^3 = 27 \equiv 1 \bmod 28$ so
$3^{90} \equiv 1^{30} \bmod 13$ thus, $3^90 \cdot 3^2 \equiv 9 \bmod 28$ therefore $3^{92} \equiv 9 \bmod 28$

If we write out an integer in base-10 notation, we can use properties of modular arithmetic to test for divisibility or congruence on the digits.

Let $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^1 a_1 + a_0$

To Test Congruence and Divisibility:

By 2: $10 \equiv 0 \bmod 2$, only the first digit is relevant, $n \equiv a_0 \bmod 2$

By 3: $10 \equiv 1 \bmod 3$ so $10^k \equiv 1 \bmod 3$ thus $n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \bmod 3$

By 4: $10 \equiv 2 \bmod 4$ and $\forall k > 1 :\ 10^k \equiv 0 \bmod 4$ so $n \equiv 2a_1 + a_0 \bmod 4$.

By 5: $10 \equiv 0 \bmod 5$, only the first digit is relevant, $n \equiv a_0 \bmod 5$

By 6: $\forall k \geq 1 :\ 10^k \equiv 4 \bmod 6$, by substitution: $n \equiv 4(a_k + \cdots + a_1) + a_0 \bmod 6$.

By 7: Suppose that $n = 10a + b$ then because $20 \equiv -1 \bmod 7$,
$10a + b \equiv 10a - 20b \bmod 7$ so if $7 \mid a - 2b$ then $7 \mid n$

By 8: $10 \equiv 2 \bmod 8$, $10^2 \equiv 4 \bmod 8$, and $\forall k > 2 :\ 10^k \equiv 0 \bmod 8$.
by substitution: $n \equiv 4a_2 + 2a_1 + a_0 \bmod 8$.

By 9: $10 \equiv 1 \bmod 9$ so $10^k \equiv 1 \bmod 9$ thus $n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \bmod 9$

By 10: $10 \equiv 0 \bmod 10$ so $n \equiv a_0 \bmod 10$

By 11: $10 \equiv -1 \bmod 11$, powers of 10 are alternately 1 and -1 modulo 10
Thus, $n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \bmod 11$

2 The Greatest Common Divisor

2.1 Definition and Properties

Definition: Let $a, b \in \mathbb{Z}$ then the greatest common divisor of a and b is a positive integer: $d \in \mathbb{Z}^+$ s.t. $d \mid a$, $d \mid b$, and $c \mid a \wedge c \mid b \implies c \mid d$

Lemma 2.1. *The greatest common divisor is unique.*

Proof. Suppose that d and d^* are greatest common divisors of a and b.
Since $d \mid a$ and $d \mid b$ the definition of d^* implies that $d \mid d^*$.
Likewise, $d^* \mid a$ and $d^* \mid b$ so $d^* \mid d$ thus $d = d^*$.

note: because of uniqueness, we can define the function: $gcd(a, b)$

Definition: If $gcd(a, b) = 1$ then a and b are coprime, relatively prime, or $a \perp b$

Lemma 2.2. $\forall a \in \mathbb{N} : a \perp a + 1$

Proof. Let $d = gcd(a, a + 1)$ then $d \mid a$ and $d \mid a + 1$. Then $d \mid 1$ so $d = 1$.

Lemma 2.3. $gcd(a, b) = gcd(a, a \pm b)$

Proof. Let $d = gcd(a, b)$ then $d \mid a$ and $d \mid b$ so $d \mid a \pm b$.
If $c \mid a$ and $c \mid a \pm b$ then $c \mid b$ so $c \mid d$. Thus, $d = gcd(a, a \pm b)$.

Lemma 2.4. *if* $a \equiv b \bmod n$ *then* $gcd(a, n) = gcd(b, n)$

Proof. Let $d = gcd(a, n)$. Since $n \mid a - b$ then $d \mid a$ and $d \mid n \implies d \mid b$.
Also if $c \mid n$ and $c \mid b$ then $c \mid a$ therefore $c \mid d$ so $d = gcd(b, n)$.

Corollary 2.5. *Since* $(a \, mod \, b) \equiv a \bmod b$ *then* $gcd(a, b) = gcd(a \, mod \, b, b)$.

The Euclidean Algorithm:
We can use the fact that $gcd(a, b) = gcd(b, a \, mod \, b)$ to find $gcd(a, b)$ recursively.
Let $b \leq a$ then $a \, mod \, b < b$ so the arguments are reduced in the recursion.
The base case is: $gcd(a, 0) = a$.

`gcd(a,b):`

1. `if` $a < b$: `return gcd(b, a)`
2. `if` $b = 0$: `return a`
3. `else: return gcd(b, a mod b)`

This algorithm requires strictly fewer than $2 \log_2(a)$ steps even in the worst case.

Theorem 2.6. *$gcd(a,b)$ is the least element of*

$$T_{a,b} = \{n \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z} : ax + by = n\}$$

Proof. $T_{a,b}$ is non-empty because $a, b \in T_{a,b}$ by well-ordering, $T_{a,b}$ has a least element: $d = ax_0 + by_0$. Use the Euclidean property to write for any x and y: $ax + by = (ax_0 + by_0)q + r$ s.t. $0 \leq r < d$. Thus, $r = a(x - x_0) + b(x - y_0)$.
If $r > 0$ then $r \in T_{a,b}$ but $r < d$, the least element. ⊠ Thus $r = 0$ and $d \mid ax + by$.

Therefore, $\forall n \in T_{a,b} : d \mid n$. $a, b \in T_{a,b}$ so $d \mid a$ and $d \mid b$.
Suppose $c \mid a$ and $c \mid b$ but because $d = ax_0 + by_0$ this implies that $c \mid d$.
Thus d satisfies the definition of the greatest common divisor. □

Corollary 2.7. *If $n = ax + by$ then $gcd(a,b) \mid n$*
Furthermore, if $gcd(a,b) \mid n$ then $n = k(ax_0 + by_0) = a(kx_0) + b(ky_0)$.
Thus $ax + by = c$ has integer solutions iff $gcd(a,b) \mid c$

Corollary 2.8. *$a \perp b$ i.e. $gcd(a,b) = 1 \iff \exists x, y \in \mathbb{Z} : ax + by = 1$*

2.2 Properties of the Greatest Common Divisor

Lemma 2.9. *$a \perp mn$ iff $a \perp m$ and $a \perp n$*

Proof. Let $a \perp m$ and $a \perp n$ then by Corollary 2.8,
$ax + my = 1$ and $ax' + ny' = 1$. Multiply: $axax' + axny' + myax' + myny' = 1$ thus $a(axx' + xny' + myx') + mnyy' = 1$. Therefore, integer solutions exist for $ax'' + mny'' = 1$ so by Corollary 2.8, $gcd(a, mn) = 1$

Let $a \perp mn$ i.e. $d \mid a, mn \implies d = 1$ then $d \mid a, m \implies d \mid mn \implies d = 1$ i.e. $a \perp m$ similarly, $d \mid a, n \implies d \mid mn \implies d = 1$ i.e. $a \perp n$.

Lemma 2.10. *If $a \perp b$, $a \mid c$, and $b \mid c$ then $ab \mid c$*

Proof. By Corollary 2.8, $ax + by = 1$. Multiply by c, $axc + byc = c$.
Since $b \mid c$ and $a \mid c$ we know that $ab \mid axc + byc$ so $ab \mid c$

Corollary 2.11. *If $m \perp n$ and $a \equiv b \bmod m$ and $a \equiv b \bmod n$*
then $m \mid a - b$ and $n \mid a - b$ so $mn \mid a - b$ i.e. $a \equiv b \bmod mn$

Lemma 2.12 (Euclid's Lemma)**.** *If $n \perp a$ and $n \mid ab$ then $n \mid b$*

Proof. Let $ab = nk$. By Corollary 2.8, $ax + ny = 1$. Multiply by b, $abx + nby = b$.
Thus by substitution, $nkx + nby = b$ so $n(kx + by) = b$ and so $n \mid b$

Corollary 2.13. *Let p be prime then for any a, either $p \mid a$ or $p \perp a$.*
Thus if $p \mid ab$ then either $p \mid a$ or $p \mid b$ (or both)

Corollary 2.14. *Let $a \perp n$. Suppose $ab \equiv ac \bmod n$*
then $n \mid a(b - c)$ so $a \mid b - c$ i.e. $b \equiv c \bmod n$

Lemma 2.15. *Let $d = gcd(a,b)$ then $\tilde{a} \perp \tilde{b}$ where $a = d\tilde{a}$ and $b = d\tilde{b}$*

Proof. By Corollary 2.7, $ax + by = d$. Because $d = gcd(a,b)$ we can write $\tilde{a}dx + \tilde{b}dy = d$ therefore $\tilde{a}x + \tilde{b}y = 1$ and so by Lemma 2.8, $\tilde{a} \perp \tilde{b}$

3 Fermat's Little Theorem

3.1 Statement of the Theorem

Theorem 3.1 (Fermat's Little Theorem). *If p is prime and $p \nmid a$ then $p \mid a^{p-1} - 1$*

Proof. Consider: ak for $1 \leq k < p$:
$p \nmid a$ and $k < p$ i.e $p \nmid k$ so by Lemma 2.12, $p \nmid ak$. Suppose $ak_1 \equiv ak_2 \bmod p$ for $1 \leq k_1, k_2 < p$ then $p \mid a(k_1 - k_2)$ so by Lemma 2.12, $p \mid k_1 - k_2$ However, $k_1 - k_2 < p$ so $k_1 = k_2$. By Theorem 1.11, $ak = pq + r$ for $0 \leq r < p$ and since $p \nmid ak$ we know that $r \neq 0$ and $ak \equiv r \bmod p$. Each ak matches to a unique r. Thus $1a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \bmod p$. Rewrite this as:
$(p-1)! a^{p-1} \equiv (p-1)! \bmod p$ i.e. $p \mid (p-1)!(a^{p-1} - 1)$. By Lemma 2.12,
$p \mid (p-1)!$ or $p \mid a^{p-1} - 1$. If $p \mid (p-1)!$ since $p \nmid p-1$ then $p \mid (p-2)!$ ect $\boxtimes$
Thus, $p \mid a^{p-1} - 1$ $\square$

Corollary 3.2. *If p is a prime then $p \mid a^p - a$ for every $a \in \mathbb{Z}$*

Proof. Suppose that $p \nmid a$ then by Fermat, $p \mid a^{p-1} - 1$ so $p \mid a^p - a$.
Otherwise, $p \mid a$ so $p \mid a(a^{p-1} - 1)$ i.e. $p \mid a^p - a$

3.2 Examples and Applications

Lemma 3.3. *Let p be prime and $p \nmid a$. If $p - 1 \mid n$ then $p \mid a^n - 1$*

Proof. Let $p - 1 \nmid n$ then $k(p-1) = n$. Also, $p \nmid a$ so by Fermat's Little Theorem, $a^{p-1} \equiv 1 \bmod p$. Thus, $a^{k(p-1)} \equiv 1 \bmod p$ so $p \mid a^n - 1$

Example: Find prime divisors of $2^{64} - 1$
Factor $64 : 1, 2, 4, 8, 16, 32, 64 \xrightarrow{+1} 2, 3, 5, 9, 17, 33, 65$. Select those factors that are one less than a prime. By the previous lemma, if a factor of 64 is one less than a prime then that prime divides $2^{64} - 1$ Thus $3, 5, 17$ are prime factors of $2^{64} - 1$.
(Not 2 because it divides the base)

Example: Find prime divisors of $10^{234} - 1$
Factor $234 : 1, 2, 3, 6, 9, 13, 18, 26, 39, 78, 117, 234 \xrightarrow{+1} 2, 3, 4, 7, 10, 14, 19, 27, 40, 79, 118, 235$.
Select those factors that are one less than a prime and do not divide 10. Thus, $3, 7, 19, 79$ are prime factors of $10^{234} - 1$

Example: Evaluate $17^{361}\ mod\ 7$
Write: $361 = 60 \cdot 6 + 1$ thus, $17^{361} = 17 \cdot (17^6)^{60}$. By Fermat's Little Theorem, $17^6\ mod\ 7 = 1$. Therefore, $17^{361}\ mod\ 7 = 17 \cdot 1 = 3$

Composite Test: either proves that a number is composite or is inconclusive.
Suppose that n is prime. Choose an a that not divisible by n then by Fermat's Little Theorem, $n \mid a^{n-1} - 1$. Thus if $n \nmid a^{n-1} - 1$ then n is composite. If $n \mid a^{n-1} - 1$ often n would have to be prime. However, as we will soon see this is not always the case.

3.3 Fermat Pseudoprimes

Definition: n is a Fermat pseudoprime for base a if $n \mid a^{n-1} - 1$ and n is composite.

Examples:

- $91 = 7 \cdot 13$ and $7, 13 \mid 3^{90} - 1$. However, $7 \perp 13$ so $7 \cdot 13 \mid 3^{90} - 1$
- $341 = 11 \cdot 31$ and $11, 31 \mid 2^{340} - 1$. However, $11 \perp 31$ so $11 \cdot 31 \mid 2^{340} - 1$
- Let $a \equiv 1 \bmod n$ or if n is odd $a \equiv -1 \bmod n$ then $a^{n-1} \equiv 1 \bmod n$

Theorem 3.4. *There exist infinitely many Fermat pesudoprimes for every base.*

Proof. For any base a we will construct a number m such that $m \mid a^{m-1} - 1$ Choose an odd prime p such that $p \nmid a$ and $p \nmid a^2 - 1$.
Define:

$$m = \frac{a^{2p} - 1}{a^2 - 1}$$

Claims:

1. $m \in \mathbb{Z}^+$.

   Proof. $a^2 \equiv 1 \bmod (a^2 - 1)$ so $a^{2p} \equiv 1 \bmod (a^2 - 1)$

2. $2p \mid m - 1$.

   Proof. $m(a^2 - 1) = a^{2p} - 1$ so $(m-1)(a^2 - 1) = a^{2p} - a^2$
   factor this as $a^2(a^{p-1} - 1)(a^{p-1} + 1)$. $p \nmid a$ so by Fermat, $p \mid a^{p-1} - 1$.
   p is odd so $p - 1 = 2k$ thus $a^{2k} \equiv 1 \bmod (a^2 - 1)$ so $a^2 - 1 \mid a^{p-1} - 1$.
   Because $p \perp a^2 - 1$ by Lemma 2.10, $p(a^2 - 1) \mid a^{p-1} - 1$.
   Either a^2 or $a^{p-1} + 1$ is even so $2 \mid a^2(a^{p-1} + 1)$.
   Thus $2p(a^2 - 1) \mid a^2(a^{p-1} - 1)(a^{p-1} + 1) = (m-1)(a^2 - 1)$ so $2p \mid m - 1$

3. $m \mid a^{m-1} - 1$.

   Proof. $m(a^2 - 1) = a^{2p} - 1$ so $a^{2p} \equiv 1 \bmod m$.
   Because $2p \mid m - 1$ by Lemma 1.7, $a^{m-1} \equiv 1 \bmod m$

4. m is composite.

   Proof.
   $$m = \frac{a^{2p} - 1}{a^2 - 1} = \frac{a^2 - 1}{a - 1} \cdot \frac{a^p + 1}{a^2 + 1}$$
   Since $a \equiv \mp 1 \bmod a \pm 1$ and p is odd, $a^p \equiv \mp 1 \bmod a \pm 1$ thus $a \pm 1 \mid a^p \pm 1$ so both factors are in $\mathbb{Z}^+$.

Since any prime greater than $a^2 - 1$ with satisfy the conditions and produce a unique pseudoprime m, there are infinitely many pseudoprimes for each base a. □

4 Divisor Sums and Perfect Numbers

Lemma 4.1. *Let p be a prime and let $p \mid a^n$ then $p \mid a$.*

Proof. Base Case: if $p \mid n^1$ then $p \mid n$.
Assume: $p \mid a^n \implies p \mid n$.
If $p \mid a^{n+1}$ then by Lemma 2.12, either $p \mid n$ or $p \mid a^n$.
By assumption, $p \mid a^n \implies p \mid a$. Thus either way, $p \mid a$.
Therefore, $p \mid a^{n+1} \implies p \mid a$ and the result holds by induction.

Theorem 4.2. *Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ with distinct $p_i \in \mathbb{P}$ then:*

1. *Let $q \in \mathbb{P}$ and $q \mid n$ then q is some p_i i.e. prime factorizations are unique.*
2. *the number of divisors of n is $\prod_{i=1}^{k}(a_i + 1)$*

Proof. Suppose that $q \mid p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ then by repeated application of Lemma 2.12, $q \mid p_i^{a_i}$ for some i. By Lemma 4.1, $q \mid p_i$ but $q, p_i \in \mathbb{P}$ so $q = p_i$.

If $d \mid n$ and $q \mid d$ then q is some p_i. Therefore, the prime factorization of d must have the same distinct primes as n but may have different powers.
Thus, $d = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ where $\forall i : 0 \leq b_i \leq a_i$. There are $a_i + 1$ possibilities for the power b_i. Therefore, the number of distinct divisors is: $\prod_{i=1}^{k}(a_i + 1)$. ☐

Definition: $\sigma(n)$ is the sum of the positive divisors of n. i.e. $\sigma(n) = \sum_{d \mid n} d$.

Lemma 4.3. *If $a \perp b$ then $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$*

Proof. write the divisors of a as $\{d_1, d_2, \dots, d_k\}$ and those of b as $\{f_1, f_2, \dots, f_r\}$.
Let $s \mid ab$ then by Lemma 2.15 we write $g = gcd(s, a)$ and $\tilde{s} \perp \tilde{a}$ and $\tilde{s}g \mid \tilde{a}gb$.
Thus, $\tilde{s} \mid \tilde{a}b$ and by Lemma 2.12, $\tilde{s} \mid b$. Since $g \mid a$ and $\tilde{s} \mid b$ and $s = \tilde{s}g$ then $s = d_i f_j$.
Thus every factor of ab is a factor of a multiplied by a factor of b.

Suppose that $d_i f_j = d_r f_s$. Let $k \mid d_i$ and $k \mid f_s$ then $k \mid a$ and $k \mid b$ but because $a \perp b$ then $k = 1$. Therefore, $d_i \perp f_s$. Similarly, $d_r \perp f_j$. Since $d_i \mid d_r f_s$ and $d_r \mid d_i f_j$. By Lemma 2.12, $d_i \mid d_r$ and $d_r \mid d_i$ so $d_i = d_r$. Similarly, $f_j = f_s$.
Therefore, no two products of divisors are equal.
So each product of divisors of a and b is a unique divisor of ab.

We can write: $\sigma(ab) = d_1 f_1 + d_2 f_1 + \dots + d_k f_1 + d_1 f_2 + \dots + d_k f_r$.
Which factors as: $\sigma(ab) = (d_1 + d_2 + \dots + d_k)(f_1 + f_2 + \dots + f_r) = \sigma(a)\sigma(b)$

Corollary 4.4. *Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ with distinct $p_i \in \mathbb{P}$ then $\sigma(n) = \sigma(p_1^{a_1})\sigma(p_2^{a_2}) \dots \sigma(p_k^{a_k})$. Also, $\sigma(p_i^{a_i}) = 1 + p_i + p_i^2 + \dots + p_i^{a_i} = \frac{p^{a_i+1}-1}{p_i-1}$. Therefore,*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

Definition: The divisor sum function partitions $\mathbb{Z}^+$ into three sets:

1. n is *abundant* if $\sigma(n) > 2n$
2. n is *perfect* if $\sigma(n) = 2n$
3. n is *deficient* if $\sigma(n) < 2n$

Proposition 4.5. *Let $p, q \in \mathbb{P}$ then p^k and (if $p, q > 2$) then pq are deficient.*

Proof. $2(p-1)p^k - p^{k+1} + 1 = p^{k+1} - 2p^k + 1 > 0$ so $2(p-1)p^k > p^{k+1} - 1$. Therefore, $2p^k > (p^{k+1} - 1)/(p-1)$ i.e. $2p^k > \sigma(p^k)$. If $p, q > 2$ then $pq - p - q - 1 > 0$ so $2pq > pq + p + q + 1 = (p+1)(q+1)$ i.e. $2pq > \sigma(pq)$. Thus there exist infinitely many both even and odd deficient numbers.

Lemma 4.6. *proper multiples of abundant and perfect numbers are abundant.*

Proof. Suppose $\sigma(n) > 2n$. For every $d \mid n$, and for any multiple by a, $ad \mid an$. Thus $\sigma(an) \geq a\sigma(n) > 2an$ so an is abundant.

Suppose that $\sigma(n) = 2n$. For every $d \mid n$, and for any proper multiple by a, $ad \mid an$. Furthermore, $a > 1$ so no $ad = 1$. Thus $\sigma(an) \geq a\sigma(n) + 1 > 2an$.

Corollary 4.7. *Because 945 is an odd abundant number, any multiple of 945 by an odd number is abundant and still odd. Therefore there are infinitely many odd abundant numbers. Furthermore, any multiple of 945 by an even number is even and abundant. Therefore there are infinitely many even abundant numbers.*

Corollary 4.8. *proper divisors of deficient and perfect numbers are deficient.*

Proof. Let a be a proper divisor of n. Suppose that a is not deficient.
Therefore it is perfect or abundant. But n is a proper multiple of a so by Proposition 4.6, n is abundant. The contrapositive of this statement is:
If n is not abundant then its proper divisors are deficient.

Theorem 4.9 (Euclid-Euler Theorem)**.** *n is an even perfect number iff $n = 2^k(2^{k+1} - 1)$ where $2^{k+1} - 1$ is prime.*

Proof. $2^k \perp 2^{k+1} - 1$ so $\sigma(2^k(2^{k+1} - 1)) = \sigma(2^k)\sigma(2^{k+1} - 1)$ but since $2^{k+1} - 1$ is prime, $\sigma(2^k)\sigma(2^{k+1} - 1) = (2^{k+1} - 1)(2^{k+1} - 1 + 1) = 2^{k+1}(2^{k+1} - 1) = 2n$.

Let $n = 2^k m$ be perfect and $2^k \perp m$. then $\sigma(2^k m) = (2^{k+1} - 1)\sigma(m)$
n is perfect so $\sigma(2^k m) = 2^{k+1}m$ and thus $(2^{k+1} - 1)\sigma(m) = 2^{k+1}m$.
$2^{k+1} - 1 \mid 2^{k+1}m$ but $2^{k+1} - 1 \perp 2^{k+1}$ so $2^{k+1} - 1 \mid m$, write: $m = r(2^{k+1} - 1)$
Thus, $(2^{k+1} - 1)\sigma(m) = 2^{k+1}r(2^{k+1} - 1)$ so $\sigma(r(2^{k+1} - 1)) = 2^{k+1}r$.
Rewrite this as $\sigma(r(2^{k+1} - 1)) = r + r(2^{k+1} - 1)$. Both terms divide $r(2^{k+1} - 1)$ and if n is even i.e. $k > 0$ the two divisors are distinct. Therefore, the only two divisors of $r(2^{k+1} - 1)$ are r and $2^{k+1} - 1$. Since 1 is a divisor of every number, $r = 1$ and thus $2^{k+1} - 1$ has only two factor so $2^{k+1} - 1$ is prime. Recombining, $n = 2^k(2^{k+1} - 1)$. ☐

Primes of the form $2^r - 1$ are known as Mersenne primes. There is a one-to-one correspondence between perfect numbers and Mersenne primes.

5 Linear Congruences

Consider congruences of the form: $ax \equiv b \bmod n$.

Lemma 5.1. *$\exists x \in \mathbb{Z}$ s.t. $ax \equiv b \bmod n$ iff $gcd(a,n) \mid b$*

Proof. Suppose $ax \equiv b \bmod n$ then $ax - b = nk$ for some $k \in \mathbb{Z}$.
Therefore, $ax - nk = b$ so $b \in T_{a,b}$ and by Corollary 2.7, $gcd(a,n) \mid b$

Let $gcd(a,n) \mid b$ then by Corollary 2.7, $\exists x, y \in \mathbb{Z}$ s.t. $ax + ny = b$.
Therefore, $ax - b = -ny$ so $ax \equiv b \bmod n$.

Lemma 5.2. *Let $g = gcd(a,n)$ then if $g \mid b$ there exist exactly g solutions up to congruence modulo n to the equation $ax \equiv b \bmod n$.*

Proof. By Lemma 2.15, $\tilde{a} \perp \tilde{n}$. Also by Lemma 5.1 there exists a solution x_0.
Suppose that $ax \equiv b \bmod n$ has two solutions x_1, x_2 then $ax_1 \equiv ax_2 \bmod n$.
Therefore, $n \mid a(x_1 - x_2)$ so $g\tilde{n} \mid g\tilde{a}(x_1 - x_2)$ and thus $\tilde{n} \mid \tilde{a}(x_1 - x_2)$.
By Lemma 2.12, $n \mid x_1 - x_2$ and thus $x_1 \equiv x_2 \bmod \tilde{n}$ and so there is exactly one solution modulo $\tilde{n}$, x_0 which is reduced modulo $\tilde{n}$.
Every solution must be of the form: $x = x_0 + \tilde{n}k$. This is a solution for any k.
$a(x_0 + \tilde{n}k) = ax_0 + \tilde{a}nk \equiv ax_0 \bmod n$. Since $x_0 < \tilde{n}$, so $x < n = \tilde{n}g$ iff $k < g$.
Therefore, if $0 \leq k < g$ then $x_0 + \tilde{n}k$ is a distinct solution modulo n.
If $x_0 + \tilde{n}k_1 \equiv x_0 + \tilde{n}k_2 \bmod n$ then $\tilde{n}g \mid \tilde{n}(k_1 - k_2)$ so $g \mid k_1 - k_2$.
Therefore, there are exactly g solutions.

Systems of Linear Congruences

Theorem 5.3 (Chinese Remainder Theorem)**.** *If $n_1, n_2, \ldots, n_k$ are pairwise coprime then the system: $x \equiv a_1 \bmod n_1$, $x \equiv a_2 \bmod n_2$, $\ldots$, $x \equiv a_k \bmod n_k$ has a unique solution modulo $n_1 n_2 \ldots n_k$*

Proof. Let $N_i = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k$. Suppose $\forall i, j : n_i \perp n_j$.
Therefore, $N_i \perp n_i$. Since $1 \mid a_i$ by Lemma 5.1, $\exists x_i \in \mathbb{Z}$ s.t. $N_i x_i \equiv a_i \bmod n_i$
However, $N_i \equiv 0 \bmod n_j$ for all $i \neq j$. Let $x = N_1 x_1 + N_2 x_2 + \cdots + N_k x_k$.
Therefore, for each i, $x \equiv a_i \bmod n_i$ and thus a solution exists.
Suppose that x_1 and x_2 solve the system. Then for each i, $x_1 \equiv x_2 \bmod n_i$.
Because $n_i \perp n_j$ by Lemma 2.11, $x_1 \equiv x_2 \bmod n_1 n_2 \ldots n_k$. □

Corollary 5.4. *Suppose that $\forall i : a_i \perp n_i$ and $\forall i \neq j : n_i \perp n_j$ then the system: $a_1 x \equiv b_1 \bmod n_1$, $a_2 x \equiv b_2 \bmod n_2$, $\ldots$, $a_k x \equiv b_k \bmod n_k$ has a unique solution modulo $n_1 n_2 \ldots n_k$*

Proof. $a_i \perp n_i$ so by Lemma 5.1 there exists z_i s.t. $a_i z_i \equiv 1 \bmod n_i$. Thus,
$x a_i z_i \equiv x \bmod n_i$. Plugging into the system, $x \equiv b_i z_i \bmod n_i$. Since the moduli are pairwise coprime, by the Chinese Remainder Theorem, there is a unique solution modulo $n_1 n_2 \ldots n_k$ to the new system. If x solves the new system: $x \equiv b_i z_i \bmod n_i$ then multiplying by a_i gives $a_i x \equiv b_i \bmod n_i$.

Corollary 5.5. *There are arbitrarily large gaps between primes.*

Proof. Let p_i be the i^{th} prime. By the Chinese Remainder Theorem:
$x \equiv -1 \bmod p_1$, $x \equiv -2 \bmod p_2$, $\ldots, x \equiv -k \bmod p_k$ has a solution modulo $p_1 p_2 \ldots p_k$. Then for each i, $p_i \mid x+i$. However, no $p_i = x+i$ else $p_{i+1} \mid p_i + 1$. A contradiction for $k > 2$. Each $x+i$ is composite so each solution begins a gap of atleast size k but k can be arbitrarily large. Alternatively, since $2, 3, 4, \ldots, n \mid n!$ then $2 \mid n!+2$, $3 \mid n!+3$, $\ldots$,$n \mid n!+n$ and thus $n!+2$, $n!+3$, $\ldots$, $n!+n$ are composite comprising a prime gap of at least size $n-1$ for arbitrarily large n.

Lemma 5.6. *Let* $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$
then $x \equiv y \bmod n$ *iff* $x \equiv y \bmod p_1^{a_1} \wedge x \equiv y \bmod p_2^{a_2} \wedge \cdots \wedge x \equiv y \bmod p_k^{a_k}$.

Proof. Suppose $x \equiv y \bmod n$ then $n \mid x-y$ and therefore, $p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} \mid x-y$. Thus, for each i, $p_i^{a_i} \mid x-y$ so $x \equiv y \bmod p_i^{a_i}$.

Suppose that $x \equiv y \bmod p_1^{a_1} \wedge x \equiv y \bmod p_2^{a_2} \wedge \cdots \wedge x \equiv y \bmod p_k^{a_k}$. Since, $p_i \perp p_j$ for $i \neq j$, we have by Corollary 2.11 that $x \equiv y \bmod p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and therefore, $x \equiv y \bmod n$.

Theorem 5.7. *The system:* $x \equiv a_1 \bmod n_1$, $x \equiv a_2 \bmod n_2$, $\ldots, x \equiv a_k \bmod n_k$ *has a solution iff* $gcd(n_i, n_j) \mid a_i - a_j$ *for each* i *and* j.

Proof. Suppose the system has a solution x. Then for any two congruences we can write: $x = a_i + n_i k_j$ and $x = a_j + n_i k_j$. Therefore, $a_i - a_j = n_j k_j - n_i k_i$. By Corollary 2.7, $gcd(n_i, n_j) \mid a_i - a_j$.

Let $\forall i, j$: $gcd(n_i, n_j) \mid a_i - a_j$ and $\{p \in \mathbb{P} \mid \exists i \text{ s.t. } p \mid n_i\} = \{p_1, p_2, \ldots, p_r\}$.
Let $n_i = p_1^{b_{i,1}} p_2^{b_{i,2}} \ldots p_r^{b_{i,r}}$. Where some $b_{i,j}$ may be zero if $p_j \nmid n_i$. Consider:

$$\begin{array}{cccc}
x \equiv a_1 \bmod p_1^{b_{1,1}} & x \equiv a_1 \bmod p_2^{b_{1,2}} & \ldots & x \equiv a_1 \bmod p_r^{b_{1,r}} \\
x \equiv a_2 \bmod p_1^{b_{2,1}} & x \equiv a_2 \bmod p_2^{b_{2,2}} & \ldots & x \equiv a_2 \bmod p_r^{b_{2,r}} \\
\vdots & \vdots & \ddots & \vdots \\
x \equiv a_k \bmod p_1^{b_{k,1}} & x \equiv a_k \bmod p_2^{b_{k,2}} & \ldots & x \equiv a_k \bmod p_r^{b_{k,r}}
\end{array}$$

Assuming that $p_j^{b_{m,j}}$ is the largest power of p_j in row j for any $p_j^{b^{i,j}}$, we have that $b^{i,j} < b^{m,j}$ and thus $x \equiv a_m \bmod p_j^{b_{i,j}}$. Since $a_m \equiv a_i \bmod gcd(n_m, n_i)$ and $p_j^{b^{i,j}} \mid n_i$ and since $b^{i,j} < b^{m,j}$ also $p_j^{b^{i,j}} \mid n_m$. Therefore, $p_j^{b^{i,j}} \mid gcd(n_i, n_m)$ so $a_m \equiv a_i \bmod p_j^{b^{i,j}}$. By transitivity, $x \equiv a_i \bmod p_j^{b_{i,j}}$ so if x solves $x \equiv a_m \bmod p_j^{b_{m,j}}$ then x solves any $x \equiv a_i \bmod p_j^{b_{i,j}}$ we can replace the column with the congruence with the largest power. Since in the reduced system each prime appears in only one equation (the one derived from that prime's column) the moduli are parwise coprime. By the Chinese Remainder Theorem, there is a solution to the reduced system. Therefore there is a solution to the full system. Since by Lemma 5.6 row i of the full solution is solved iff $x \equiv a_i \bmod n_i$ and the full system has a solution so the original system must also be solved by x. $\square$

6 Euler's Φ Function and Primitive Roots

6.1 Euler's Function and Theorem

Definition: $\Phi(n) = \{x \in \mathbb{N} \mid x < n \land x \perp n\}$ and $\phi(n) = |\Phi(n)|$

Lemma 6.1. *if $a \perp b$ then $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$*

Proof. Consider the system: $x \equiv k \bmod a$ and $x \equiv g \bmod y$.
Since $a \perp b$, by the Chinese Remainder Theorem there exists a solution less than ab.
Suppose the solution x solves a different system $x \equiv k' \bmod a$ and $x \equiv g' \bmod y$.
Then by transitivity, $k \equiv k' \bmod a$ and $g \equiv g' \bmod b$ so no two system have the same solution so each reduced pair (g, k) corresponds to exactly one $x < ab$.
By Lemma 2.4 $k \perp a$ and $g \perp b$ is equivalent to $x \perp a$ and $x \perp b$.
Also, by Lemma 2.9, $x \perp a$ and $x \perp b$ is equivalent to $x \perp ab$.
Therefore, $k \perp a$ and $g \perp b \iff x \perp ab$. There are $\phi(ab)$ such x and $\phi(a)\phi(b)$ such pairs (k, g) so $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Theorem 6.2. $\sum_{d|n} \phi(d) = n$

Proof. Define:

$$A_g = \{a \in \mathbb{Z}^+ \mid a \leq n \land gcd(a, n) = g\}$$

By Lemma 2.15, $a \in A_g$ iff $\tilde{a} \perp \tilde{n}$ and $\tilde{a} \leq \tilde{n}$ where $\tilde{a}g = a$, $\tilde{n}g = n$.
Thus, $|A_g| = \phi(\tilde{n})$. Alternatively, for $d \mid n$ we have that $\phi(d) = |A_{\frac{n}{d}}|$.
Each number has exactly one gcd so the sets A_g for each $g \mid n$ partition $\{1, 2, \cdots, n\}$.
Therefore, $\sum_{g|n} |A_g| = n$ and so $\sum_{d|n} \phi(d) = n$ □

Corollary 6.3. *If $p \in \mathbb{P}$ then for $k \in \mathbb{Z}^+$, $\phi(p^k) = p^k - p^{k-1}$*

Proof. p^k has factors $1, p, p^2, \cdots, p^k$ and so by Theorem 6.2,
$p^k = \phi(p^k) + \phi(p^{k-1}) + \cdots + \phi(1)$ and $p^{k-1} = \phi(p^{k-1}) + \phi(p^{k-2}) + \cdots + \phi(1)$.
Therefore, $p^k - p^{k-1} = \phi(p^k)$.

Corollary 6.4. *p is prime iff $\phi(p) = p - 1$*

Proof. Suppose that $\phi(n) = n - 1$ and $n = ab$ where $a < n$ then because every $0 < k < n$ must be coprime to n because $\phi(n) = n - 1$, then $a \perp n$. However, $a \mid a$ and $a \mid n$ thus $a = 1$ so n is prime. By Corollary 6.3, if p is prime then $\phi(p) = p - 1$

Proposition 6.5. $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ *for $p \in \mathbb{P}$*

Proof. Let $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ for distinct primes. Then by Lemma 6.1,
$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \ldots \phi(p_k^{a_k})$. Also, by Corollary 6.3, $\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right)$. Thus, $\phi(n) = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$.
Because $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ then $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$

Corollary 6.6. $\phi(ab) = \phi(a)\phi(b)\dfrac{g}{\phi(g)}$ *where* $g = gcd(a,b)$

Proof. If $p \mid ab$ then by Lemma 2.12, $p \mid a$ or $p \mid b$ or both. Thus to remove double counting, $\phi(ab) = ab\prod_{p|ab}\left(1-\dfrac{1}{p}\right) = a\prod_{p|b}\left(1-\dfrac{1}{p}\right)\cdot b\prod_{p|b}\left(1-\dfrac{1}{p}\right)\cdot\prod_{p|a,b}\left(1-\dfrac{1}{p}\right)^{-1}$.

However, $\dfrac{\phi(g)}{g} = \prod_{p|a,b}\left(1-\dfrac{1}{p}\right)$ so $\phi(ab) = \phi(a)\phi(b)\dfrac{g}{\phi(g)}$.

Lemma 6.7. *If* $a \mid b$ *then* $\phi(a) \mid \phi(b)$

Proof. Let $b = ak$ then by Lemma 6.6, $\phi(b) = \phi(a)\phi(k)\dfrac{g}{\phi(g)}$

Thus, $\phi(b) = \phi(a)\; k \prod_{p|k \wedge p\nmid a}\left(1-\dfrac{1}{p}\right)$ and therefore, $\phi(a) \mid \phi(b)$

Corollary 6.8. *If* $n > 2$ *then* $\phi(n)$ *is even.*

Proof. Suppose $p \mid n$ where p is an odd prime.
Then $\phi(p) \mid \phi(n)$. However, $\phi(p) = p - 1$ is even so $\phi(n)$ is even.
Else, $n = 2^k$ so $\phi(n) = 2^k - 2^{k-1}$ which is even if $k > 1$ i.e. $n > 2$.

Theorem 6.9 (Euler's Theorem)**.** *if* $a \perp n$ *then* $a^{\phi(n)} \equiv 1 \bmod n$

Proof. Enumerate the elements of $\Phi(n)$ as $b_1, b_2, \cdots, b_{\phi(n)}$. Let $a \perp n$. Suppose that $ab_i \equiv ab_j \bmod n$ then by Corollary 2.14, $b_i \equiv b_j \bmod n$ so the elements ab_i are distinct.
$a \perp n$ and $b_i \perp$ so by Lemma 2.9, $ab_i \perp n$. Thus $(ab_i\, mod\, n) \perp n$ so $ab_i\, mod\, n \in \Phi(n)$.
Therefore, $\exists b_j \in \Phi(n)$ s.t. $ab_i \equiv b_j \bmod n$. Since the ab_i are distinct modulo n, $ab_1, ab_2, \cdots, ab_{\phi(n)}$ is a permutation of $b_1, b_2, \cdots, b_{\phi(n)}$ modulo n.
In particular, $ab_1ab_2\cdots ab_{\phi(n)} \equiv b_1b_2\cdots b_{\phi(n)} \bmod n$. And thus,
$a^{\phi(n)}b_1b_2\cdots b_{\phi(n)} \equiv b_1b_2\cdots b_{\phi(n)} \bmod n$. Since every $b_i \perp n$,
by repeated application of Corollary 2.14, $a^{\phi(n)} \equiv 1 \bmod n$. ☐

Fermat's Little Theorem is the special case of Euler's Theorem
where if p is prime then $\phi(p) = p - 1$ and $p \perp a$ whenever $p \nmid a$.

RSA Encryption Select large distinct primes p and q and let the modulus $n = pq$.
Generate an encryption key e coprime with $\phi(n)$. Next, Lemma 2.7 implies that a decryprion key d exists such that $ed = \phi(n)r + 1$ for $d, r > 0$.
Publish the encryption key and modulus but keep the decryption key secret.
To send a message, use a standard scheme to code that message as an integer $m \in \Phi(n)$. Then use the public encryption key and modulus to send out cypher-text $c = m^e\, mod n$. Exponentiate the cypher-text using the private description key, $c^d = m^{ed} = m \cdot m^{\phi(n)r}$. Since $m \perp n$ by Euler's Theorem, $m^{\phi(n)} \equiv 1 \bmod n$ so $m \cdot m^{\phi(n)r} \equiv m \bmod n$ and thus, $c^d \equiv m \bmod n$. The message has been decrypted.
RSA is secure because to calculate d requires knowledge of $\phi(n)$. In general this is an extremely computationally expensive problem. However, beginning with the prime factorization $n = pq$, the computation: $\phi(n) = (p-1)(q-1)$ becomes trivial.

6.2 Order and Primitive Roots

Definition: Let $g \perp n$ then $ord_n(g)$ is the least positive r s.t. $g^r \equiv 1 \bmod n$.

Lemma 6.10. *If* $g^s \equiv 1 \bmod n$ *then* $ord_n(g) \mid s$.

Proof. By the Euclidean Property, $s = ord_n(g)q + r$ for $0 \leq r < ord_n(g)$.
Since $g^{ord_n(g)} \equiv 1 \bmod n$ therefore $g^s = (g^{ord_n(g)})^q \cdot g^r \equiv g^r \bmod n$.
However, $g^s \equiv 1 \bmod n$ so $g^r \equiv 1 \bmod n$ but $r < ord_n(g)$ the least positive exponent.
Therefore, $r = 0$ and thus, $ord_n(g) \mid s$.

Corollary 6.11. *If* $g \perp n$ *then* $ord_n(g) \mid \phi(n)$

Proof. By Euler's Theorem, $g \perp n$ implies that $g^{\phi(n)} \equiv 1 \bmod n$.
Therefore, by Lemma 6.10, $ord_n(g) \mid \phi(n)$

Lemma 6.12. *If* $x \equiv y \bmod n$ *then* $ord_n(x) = ord_n(y)$.

Proof. Let $x \equiv y \bmod n$ then by Lemma 1.7, $x^s \equiv y^s \bmod n$.
Therefore, $x^s \equiv 1 \bmod n \iff y^s \equiv 1 \bmod n$ so the least exponents are equal.

Proposition 6.13. $n \mid \phi(a^n - 1)$

Proof. $ord_{a^n-1}(a) = n$ because if $r < n$ then $a^r - 1 < a^n - 1$.
Thus by Lemma 6.11, $n \mid \phi(a^n - 1)$

Lemma 6.14. $ord_n(g^k) = ord_n(g)/gcd(k, ord_n(g))$

Proof. Let $s = ord_n(g^k)$ and $ord_n(g) = r$. Since $(g^k)^r = g^{kr} \equiv 1 \bmod n$ then $s \mid r$.
Let $r = ds$. $(g^k)^s \equiv 1 \bmod n$ then $r \mid ks$ thus, $ds \mid ks$ so $d \mid k$. Suppose that $c \mid k$ and $c \mid r$ then $(g^k)^{r/c} = (g^r)^{k/c} \equiv 1 \bmod n$ therefore $sc \mid r$ i.e. $cs \mid ds$ and thus $c \mid d$.
Collectively, $d \mid r$ and $d \mid k$ and $c \mid k \wedge c \mid r \implies c \mid d$ therefore $d = gcd(k, r)$
However, $r = ds$ so therefore, $ord_n(g) = gcd(g, ord_n(g)) \cdot ord_n(g^k)$

Definition: g is a primitive root modulo n if $g \perp n$ and $ord_n(g) = \phi(n)$.

Proposition 6.15. *If* g *is a primitive root modulo* n *then* $\{g^k mod n \mid k \in \mathbb{Z}^+\} = \Phi(n)$

Proof. Let since $g \perp n$ by Lemma 2.4, $g^k \, mod \, n \perp n$ so for every k, $g^k \, mod \, n \in \Phi(n)$.
Suppose that $g^i \equiv g^j \bmod n$ for $i < j < \phi(n)$ then $g^i \cdot g^{\phi(n)-j} \equiv g^j \cdot g^{\phi(n)-j} \bmod n$ but by Euler's Theorem $g^j \cdot g^{\phi(n)-j} = g^{\phi(n)} \equiv 1 \bmod n$ and thus $g^{\phi(n)+i-j} \equiv 1 \bmod n$ but $\phi(n) + i - j < \phi(n)$ contradicting $ord_n(g) = \phi(n)$. Therefore there are atleast $\phi(n)$ elements of $\{g^k \, mod \, n \mid k \in \mathbb{Z}^+\} \subset \Phi(n)$ and therefore, $\{g^k \, mod \, n \mid k \in \mathbb{Z}^+\} = \Phi(n)$

Lemma 6.16. *If* $d \mid \phi(n)$ *then either* $|\{x \in \Phi(n) \mid ord_n(x) = d\}| \geq \phi(d)$ *or is zero. In particular, if* $\Phi(n)$ *contains a primitive root then the are exactly* $\phi(\phi(n))$ *in* $\Phi(n)$.

Proof. Suppose that $\{x \in \Phi(n) \mid ord_n(x) = d\}$ is not empty. Then $\exists g \in \Phi(n)$ s.t. $ord_n(g) = d$. Consider $ord_n(g^k)$ by Lemma 6.14, $ord_n(g^k) = d$ iff $gcd(k, d) = 1$. Furthermore, for $s, t < d$ if $g^s \equiv g^t \bmod n$ then $s = t$ so exponents less that d give distinct elements. There are $\phi(d)$ exponents k s.t. $k \perp d$ and $k < d$ this gives a lower bound on the number of elements with order d.
Let $d = \phi(n)$ and let a primitive root g exist. By Proposition 6.15, there are no elements other than g^k in $\Phi(n)$ so there are exactly $\phi(\phi(n))$ elements of order $\phi(n)$.

6.3 The Primitive Root Theorem

Theorem 6.17 (Lagrange's Polynomial Theorem)**.** *If p is a prime and $f(x)$ is a polynomial of order n with a leading coefficient not divisible by p then $f(x) \equiv 0 \bmod p$ has at most n distinct solutions modulo p.*

Proof. Base Case: for $n = 0$, $a_0 \equiv 0 \bmod p$ has zero solutions if $p \nmid a_0$.
Assume the theorem holds for degree n polynomials. Let f have degree $n+1$ and have a non-zero leading coefficient modulo p. Suppose $p \mid f(r)$ then $f(x) = (x-r)g(x)+pk$ where g has degree n. g cannot have a leading coeficient divisible by p because then $f(x) = (x-r)g(x) + kp$ would as well. If $p \mid f(x)$ then $p \mid (x-r)g(x)$ so by Lemma 2.12, $p \mid x - r$ or $p \mid g(x)$. Suppose that $p \mid x_1 - r$ and $p \mid x_2 - r$ then $p \mid x_1 - x_2$ so the solutions are congruent. Since g has degree n, by hypothesis there are at most n solutions to $p \mid g(x)$. Therefore, including r, there are at most $n + 1$ solutions to $p \mid f(x)$. The result holds for all degrees by induction. $\square$

Theorem 6.18. *If p is prime then if $d \mid p-1$ there are exactly $\phi(d)$ elements of $\Phi(p)$ with order d. In particular, there are $\phi(p-1)$ primitive roots.*

Proof. Suppose that $\exists g \in \Phi(p)$ s.t. $ord_p(g) = d$. Then $x^d - 1 \equiv 0 \bmod p$ has a solution g. Furthermore, g^i for $0 \leq i < d$ are also solutions and are distinct because $ord_p(g) = d$ and each exponent is less than d (see Proposition 6.15). These are d distinct solutions to a degree d polynomial so by Theorem 6.17, there are no others. If $ord_p(x) = d$ then $x^d - 1 \equiv 0 \bmod p$ so there is some k s.t. $x = g^k$. By Lemma 6.14, $ord_p(g^k) = d$ iff $gcd(k, d) = 1$. Therefore, there are exactly $\phi(d)$ such k and by extension exactly $\phi(d)$ such x.

However, this proof presupposes that at least one element of order d exists.
Let $S_d = \{x \in \Phi(p) \mid ord_n(x) = d\}$ if S_d is non-empty then $|S_d| = \phi(d)$.
Therefore, either $|S_d| = 0$ or $|S_d| = \phi(d)$. Every element of $\Phi(p)$ has exactly one order and therefore the sets S_d partition $\Phi(p)$. In particular if any $|S_d| = 0$ then

$$\sum_{d|p-1} |S_d| = \phi(p) = p - 1 < \sum_{d|p-1} \phi(d)$$

However, by Theorem 6.2, $\sum_{d|p-1} \phi(d) = p - 1$ so for every d, $|S_d| = \phi(d)$ $\square$

Lemma 6.19. *Let n be odd. For each primitive root modulo n there is a primitive root modulo $2n$. Also, $\Phi(n)$ and $\Phi(2n)$ contain the same number of primitive roots. In particular, if primitive roots exist modulo n then primitive roots exist modulo $2n$.*

Proof. Because $2 \perp n$, $\phi(2n) = \phi(2) \cdot \phi(n) = \phi(n)$. Chose g to be an odd primitive root modulo n. If g is even then choose $g + n$ which is odd but has equal order. $g \perp 2$ and $g \perp n$ so by Lemma 2.9, $g \perp 2n$. By Euler's Theorem, $g^{\phi(2n)} \equiv 1 \bmod 2n$. However, if $k < \phi(n) = \phi(2n)$ then $n \nmid g^k - 1$ because $ord_n(g) = \phi(n)$ and thus $2n \nmid g^k - 1$ so if $k < \phi(2n)$ then $g^k \not\equiv 1 \; mod \; 2n$. Thus, $ord_{2n}(g) = \phi(2n)$ i.e. g is a primitive root modulo $2n$. Since $\phi(2n) = \phi(n)$, by Lemma 6.16, both $\Phi(2n)$ and $\Phi(n)$ contain $\phi(\phi(n))$ primitive roots.

Theorem 6.20 (The Primitive Root Theorem)**.** *There exist primitive roots modulo:* $2, 4, p^k$*, and* $2p^k$ *where* p *is an odd prime and not for any other moduli.*

Proof. Let p be an odd prime. Claims:

1. $\exists g$ s.t. $ord_p(g) = \phi(p)$ and $g^{\phi(p)} \not\equiv 1 \, mod \, p^2$

   Proof. By Theorem 6.18, there exists a primitive root, x modulo p. Suppose that $x^{\phi(p)} \equiv 1 \bmod p^2$ Then, $(x+p)^{\phi(p)} = x^{\phi(p)} + \phi(p)x^{\phi(p)-1}p + \cdots + p^{\phi(p)}$ However, $p \nmid \phi(p)$ and $p \nmid x^{\phi(p)-1}$ thus $p \nmid \phi(p)x^{\phi(p)-1}$ therefore, $p^2 \nmid \phi(p)x^{\phi(p)-1}p$ thus $(x+p)^{\phi(p)} \not\equiv 1 \, mod \, p^2$ Furthermore, $x + p \equiv x \bmod p$ so $x + p$ is also a primitive root modulo p. Choose $g = x + p$ otherwise choose $g = x$.

2. $\forall k \geq 1 : \; g^{\phi(p^k)} \not\equiv 1 \, mod \, p^{k+1}$

   Proof. By Euler's Theorem, $g^{\phi(p^k)} = 1 + mp^k$. Let $g^{\phi(p^k)} \not\equiv 1 mod p^{k+1}$ i.e. $p \nmid m$. $\phi(p^{k+1}) = p^k(p-1) = p\phi(p^k)$. Thus, $g^{\phi(p^{k+1})} = g^{p\phi(p^k)} = (1 + mp^k)^p$. Expand, $(1 + mp^k)^p = 1 + mp^{k+1} + \cdots + (mp^k)^p$ but $p \nmid m$ so $g^{\phi(p^{k+1})} \not\equiv 1 \, mod \, p^{k+2}$. Since, $g^{\phi(p)} \not\equiv 1 \, mod \, p^2$ by Induction the result holds for all $k \geq 1$.
   The induction only holds if $kp > k + 1$. However, for $p = 2$ and $k = 1$ this is false: $g^{\phi(2^2)} = (1+2m)^2 = 1 + 2^2 m + 2^2 m^2$ but $2 \mid m + m^2$ so $2^3 \mid (1+2m)^2 - 1$. Therefore, $g^{\phi(2^2)} \equiv 1 \bmod 2^3$ although $g^{\phi(2^1)} \not\equiv 1 \, mod \, 2^2$

3. $\forall k \geq 1 : ord_{p^k}(g) = \phi(p^k)$ i.e. g is a primitive root for p^k

   Proof. Assume: $ord_{p^k}(g) = \phi(p^k)$. Let $m = ord_{p^{k+1}}(g)$. Then $p^k \mid p^{k+1} \mid g^m - 1$ Thus, $ord_{p^k}(g) = \phi(p^k) \mid m$. Also, $m \mid \phi(p^{k+1})$ so $\phi(p^k) \mid m \mid \phi(p^k)p$ thus, $m = \phi(p^k)$ or $\phi(p^{k+1})$. However, $g^{\phi(p^k)} \not\equiv 1 \, mod \, p^{k+1}$ so $ord_{p^{k+1}}(g) = \phi(p^{k+1})$ By induction, the result holds for all k.

4. If $a, b > 2$ and $a \perp b$ then no primitive roots exist modulo $n = ab$

   Proof. If $g \perp ab$ then $g \perp a$ and $g \perp b$ so by Euler's Theorem, $g^{\phi(a)} \equiv 1 \bmod a$ and $g^{\phi(b)} \equiv 1 \bmod b$. Since $a, b > 2$ by Corollary 6.8, $2 \mid \phi(a)$ and $2 \mid \phi(b)$. Therefore, $g^{\phi(a)\cdot\phi(b)/2} \equiv 1 \bmod a$ and $g^{\phi(b)\cdot\phi(a)/2} \equiv 1 \bmod b$. Since $a \perp b$ by Corollary 2.11, $g^{\phi(a)\cdot\phi(b)/2} \equiv 1 \bmod ab$ and $\phi(ab) = \phi(a) \cdot \phi(b)$. Thus, $\phi(a) \cdot \phi(b)/2 < \phi(n)$ so $\forall g \in \Phi(n) : ord_n(g) < \phi(n)$ i.e. no primitive roots modulo n exist.

5. There exist primitive roots modulo 2^k only for 2 and 4

   Proof. 1 and 3 are primitive roots for 2 and 4 respectively. However, $\forall g : \; g^{\phi(2^2)} \equiv 1 \bmod 2^3$. Let $\forall g : \; g^{\phi(2^k)} \equiv 1 \bmod 2^{k+1}$ i.e. $g^{\phi(2^k)} = 1 + m2^{k+1}$ $g^{\phi(2^{k+1})} = (1 + m2^{k+1})^2 = 1 + m2^{k+2} + m^2 2^{2k+2} \equiv 1 \bmod 2^{k+2}$ thus by induction: $\forall g : \; g^{\phi(2^k)} \equiv 1 \bmod 2^{k+1}$ in particular, $\forall g : ord_{2^{k+1}}(g) \leq \phi(2^k) < \phi(2^{k+1})$

Primitive roots exist modulo 2, 4, and, p^k. By Lemma 6.19, there also exist primitive roots modulo $2p^k$ because p is odd. If $n \neq 2, 4, p^k, 2p^k$ then $n = 2^k > 4$ or n has coprime factors besides 2 and thus there do not exist primitive roots modulo n. □

7 Quadratic Residues

Definition: a is a quadratic residue modulo p if $p \nmid a$ and $\exists x$ s.t. $x^2 \equiv a \bmod p$

Lemma 7.1 (Euler's Criterion)**.** *Let p be an odd prime and $p \nmid a$ then a is a quadratic residue modulo p iff $a^{(p-1)/2} \equiv 1 \bmod p$.*

Proof. Let g be a primitive root modulo p. Then $a \equiv g^m \bmod p$.
Thus, $a^{(p-1)/2} = g^{m(p-1)/2} \equiv 1 \bmod p$. $ord_p(g) = p-1$ so $p-1 \mid m(p-1)/2$ thus, $2(p-1) \mid m(p-1)$ so $2 \mid m$. Thus, $a \equiv (g^{m/2})^2 \bmod p$ so a is a quadratic residue.
Suppose a is a quadratic residue then $a \equiv x^2 \bmod p$. Write $x \equiv g^n \bmod p$ then $a \equiv g^{2n} \bmod p$ therefore, $a^{(p-1)/2} = g^{n(p-1)} \equiv 1 \bmod p$.

Definition: The Legendre Symbol:

- $(a|p) = 1$ if a is a quadratic residue modulo p
- $(a|p) = -1$ if a is a quadratic non-residue modulo p
- $(a|p) = 0$ if $p \mid a$

Lemma 7.2. *If p is an odd prime then $(a|p) \equiv a^{(p-1)/2} \bmod p$*

Proof. If $p \mid a$ then $p \mid a^{(p-1)/2}$ so $a^{(p-1)/2} \equiv 0 \bmod p$ and $(a|p) = 0$. Else, $p \nmid a$ so by Fermat's Little Theorem, $p \mid a^{p-1} - 1$ since p is odd, $p \mid (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$. Thus, $p \mid a^{(p-1)/2} - 1$ or $p \mid a^{(p-1)/2} + 1$. If a is a quadratic residue modulo p then both $(a|p) = 1$ and $a^{(p-1)/2} \equiv 1 \bmod p$. If a is a quadratic non-residue, $p \nmid a^{(p-1)/2} - 1$ so $p \mid a^{(p-1)/2} + 1$ i.e. $a^{(p-1)/2} \equiv -1 \bmod p$ but also $(a|p) = -1$.

Lemma 7.3. $(ab|p) = (a|p) \cdot (b|p)$

Proof. $(a|p) \equiv a^{(p-1)/2} \bmod p$ and $(b|p) \equiv b^{(p-1)/2} \bmod p$ thus
$(a|p)(b|p) \equiv a^{(p-1)/2} \cdot a^{(p-1)/2} \bmod p$ but $(ab|p) \equiv (ab)^{(p-1)/2} \bmod p$ so $(ab|p) \equiv (a|p)(b|p) \bmod p$ but the values are $\{-1, 0, 1\}$ and $p > 2$ so $(ab|p) = (a|p)(b|p)$

Lemma 7.4. *If $a \equiv b \bmod p$ then $(a|p) = (b|p)$*

Proof. $a \equiv b \bmod p$ so $a^{(p-1)/2} \equiv b^{(p-2)/2} \bmod p$ thus $(a|p) \equiv (b|p) \bmod p$ but the values are $\{-1, 0, 1\}$ and $p > 2$ so $(a|p) = (b|p)$

Proposition 7.5. -1 *is a quadratic residue modulo p iff $p \equiv 1 \bmod 4$*

Proof. $(-1|p) \equiv (-1)^{(p-1)/2} \bmod p$ thus $(-1|p) = 1$ iff $\frac{p-1}{2} = 2k$ i.e. $p = 4k + 1$

Proposition 7.6. *There are infinitely many primes of the form $4k + 1$*

Proof. Let $p \mid (n!)^2 + 1$. Because $(n!)^2 \equiv -1 \bmod p$ then $(-1|p)$ so $p = 4k + 1$. However, if $p \leq n$ then $p \mid n!$ implying that $p \mid 1$ ⊠ Thus, $p > n$. Therefore there are arbitrarily large primes of the form $4k + 1$ and thus no upper bound.

Proposition 7.7. *There are infinitely many primes of the form $4k - 1$*

Proof. Suppose that $p_1, p_2, \ldots, p_r$ were all the primes of the form $4k - 1$. Consider, $N = 4(p_1 \cdot p_2 \cdot \ldots \cdot p_r) - 1$. No $p_i \mid N$ else $p_i \mid -1$. Thus, every prime divisor of N has the form $4k+1$. If $p \equiv q \equiv 1 \bmod 4$ then $pq \equiv 1 \bmod 4$ however, $N \equiv -1 \bmod 4$ ⊠

Lemma 7.8 (Gauss's Lemma). *Let p be an odd prime s.t. $p \nmid a$ and n be the number of residues modulo p of $1\cdot a, 2\cdot a, \ldots, \frac{p-1}{2}\cdot a$ that are greater than $\frac{p-1}{2}$ then $(a|p) = (-1)^n$*

Proof. Suppose that $xa \equiv ya \bmod p$ because $p \nmid a$ by Corollary 2.14, $x \equiv y \bmod p$. If $ax \ mod\ p = r > \frac{p-1}{2}$ then $p - r < \frac{p-1}{2}$ and $-(p-r) \equiv ax \bmod p$. Suppose that $-ax \equiv ay \bmod p$ then $p \mid x+y$, impossible because $x, y < \frac{p-1}{2}$. Each ax reduces upto sign to a unique $r < \frac{p-1}{2}$ Thus, $1a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a \equiv (-1)^n \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \bmod p$ However, $1a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a = a^{(p-1)/2} \cdot (\frac{p-1}{2})!$ therefore, $a^{(p-1)/2} \cdot (\frac{p-1}{2})! \equiv (-1)^n \cdot (\frac{p-1}{2})! \bmod p$ so $a^{(p-1)/2} \equiv (-1)^n \bmod p$. Furthermore, $a^{(p-1)/2} \equiv (a|p) \bmod p$ thus $(a|p) = (-1)^n$

Theorem 7.9 (Quadratic Reciprocity). *If p and q are distinct odd primes then*

$$(p|q)(q|p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Proof. Let $a = \frac{p-1}{2}$ and $b = \frac{q-1}{2}$. For each $r < pq$ there is a unique (x, y) s.t. $r \equiv x \bmod p$ and $r \equiv y \bmod q$ with $x < p$ and $y < q$. Let $f(r) = (x, y)$ where f is a bijection by the Chinese Remainder Theorem. Let $P = f([1, \frac{pq-1}{2}])$ and let u be the number of $r \in P$ s.t. $f(r) = (x, 0)$ for $x > a$ and v, the number of r s.t. $f(r) = (0, y)$ for $y > b$. Consider:

$$N_1 = |\{(x, y) \in P \mid 0 < x \leq a \wedge 0 < y \leq b\}|$$
$$N_2 = |\{(x, y) \in P \mid a < x < p \wedge 0 \leq y \leq b\}|$$
$$N_3 = |\{(x, y) \in P \mid 0 \leq x \leq a \wedge b < y < q\}|$$

$\frac{pq-1}{2} = \frac{(p-1)q}{2} + \frac{q-1}{2} = aq + b$. Thus $r = lq + k < aq + b$ for $0 \leq l \leq a$ and $1 \leq k \leq b$. Furthermore, $r \equiv k \bmod q$ so there are $(a+1)b$ elements of P s.t. $0 < y \leq b$ also there are $b - v$ elements of P s.t. $x = 0$ and $0 \leq y \leq b$ also there are u elements of P s.t. $a < x < p$ and $y = 0$ thus $N_1 + N_2 = (ab + b) - (b - v) + u = ab + u + v$
Swapping q for p the same argument shows that $N_1 + N_3 = ab + u + v$.
Let $f(r) = (x, y)$ with $1 \leq x \leq a$ and $1 \leq y \leq b$. $f(pq - r) = (p - x, q - y)$ then exactly one of $(x, q-y)$ and $(p-x, y)$ is in P. There are ab such x and y. When $x = 0$ there are v such $y > b(N_3)$ and when $y = 0$ there are u such $x > a(N_2)$. Therefore, $N_2 + N_3 = ab + u + v$. Summing: $2(N_1 + N_2 + N_3) = 3(ab + u + v)$ thus $2 \mid ab + u + v$ so $(-1)^{ab+u+v} = 1$ multiplying by $(-1)^{u+v}$ gives $(-1)^{ab} = (-1)^u \cdot (-1)^v$. Furthermore, if $f(r) = (x, 0)$ then $r = kq$ where $k \leq a$ because $((a+1)q > aq + b)$ so u is the number of $1 \cdot q, 2 \cdot q, \ldots, a \cdot q$ which are greater than a modulo p thus by Gauss's Lemma, $(-1)^u = (q|p)$ likewise $(-1)^v = (p|q)$. Thus, $(p|q)(q|p) = (-1)^{ab} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ ☐

Proposition 7.10. 2 *is a quadratic residue modulo p iff $p \equiv \pm 1 \bmod 8$*

Proof. By Gauss's Lemma, $(2|p) = (-1)^n$ where n is the number of elements, $2, 4, \ldots, p-1$ that are greater than $\frac{p-1}{2}$. If $\frac{p-1}{2}$ is even then $n = \frac{p-1}{4}$ thus $(2|p) = 1$ iff $2 \mid n$ i.e. $p \equiv 1 \bmod 8$. If $\frac{p-1}{2}$ is odd then n counts the middle element i.e. $n = \frac{1}{2}(\frac{p-1}{2} + 1) = \frac{p+1}{4}$ thus $(2|p) = 1$ iff $2 \mid n$ i.e. $p \equiv -1 \bmod 8$.

8 Special Families of numbers

This section is devoted to a survey of a selection of the most important families of numbers that have been areas of theoretical and applied research in number theory.

8.1 Carmichael Numbers

Lemma 8.1. *If $n \mid a^k \pm 1$ then $a \perp n$*

Proof. Let $a^k \pm 1 = ng$ or $a(\mp a^{k-1}) + n(\pm g) = 1$ so there exist integer solutions to the equation: $ax + ny = 1$ and thus by Corollary 2.7 $a \perp n$.

Definition: a Carmichael number is a composite number n such that
$\forall a \in \mathbb{Z}^+ : a \perp n \implies n \mid a^{n-1} - 1$.
Equivalently, n is a pseduoprime for every base a for which $a \perp n$.

Theorem 8.2 (Korselt's Criterion)**.** *n is a Carmichael number iff n is composite and $\forall p \in \mathbb{P} : p \mid n \implies p - 1 \mid n - 1$ and n is square-free i.e. $\nexists\, p \in \mathbb{P}$ s.t. $p^2 \mid n$*

Proof. Let n be square-free i.e the product of distinct primes: $n = p_1 p_2 \dots p_k$
Let $a \perp n$ therefore for each prime divisor p of n, $p \nmid a$. Therefore by Fermat's Little Theorem, $p \mid a^{p-1} - 1$. Since $p-1 \mid n-1$ this implies that $p \mid a^{n-1} - 1$ for each $p \mid n$. Because distinct prime are coprime, by Lemma 2.10: $p_1 p_2 \dots p_k \mid a^{n-1} - 1$ so $n \mid a^{n-1} - 1$ for each $a \perp n$ and by hypothesis n is composite.

Suppose that n is a Carmichael number.
Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ with distinct $p_i \in \mathbb{P}$. For any particular p_i,
by The Primitive Root Theorem, there exists a number, g, s.t. $ord_{p_i}(g) = p_i - 1$.
Consider the system:

$$x \equiv 1 \bmod p_1 \ , \ x \equiv 1 \bmod p_2 \ , \dots , \ x \equiv g \bmod p_i \ , \dots , \ x \equiv 1 \bmod p_k$$

he primes are distinct and thus are coprime so there exists a solution by the Chinese Remainder Theorem. $x \perp n$ because for every $p \mid n$ we have that $p \nmid x$.
Thus because n is Carmichael, $n \mid x^{n-1} - 1$ therefore, $p_i \mid x^{n-1} - 1$. Since $g \equiv x \bmod p_i$ by Lemma 6.12, $ord_{p_i}(x) = ord_{p_i}(g) = p_i - 1$ and so Lemma 6.10 implies that $p_i - 1 \mid n - 1$. Thus if $p \mid n$ then $p - 1 \mid n - 1$.

Suppose that some $p_i^2 \mid n$. The Primitive Root Theorem implies that there exists a number, g, s.t. $ord_{p_i^2}(g) = p_i(p_i - 1)$. Consider the system:

$$x \equiv 1 \bmod p_1 \ , \ x \equiv 1 \bmod p_2 \ , \dots , \ x \equiv g \bmod p_i^2 \ , \dots , \ x \equiv 1 \bmod p_k$$

The primes are distinct and thus are coprime so there exists a solution by the Chinese Remainder Theorem. $x \perp n$ because for every $p \mid n$ we have that $p \nmid x$.
Thus because n is Carmichael, $n \mid x^{n-1} - 1$ therefore, $p_i^2 \mid x^{n-1} - 1$.
Since $g \equiv x \bmod p_i^2$ by Lemma 6.12, $ord_{p_i^2}(x) = ord_{p_i^2}(g) = p_i(p_i - 1)$ and so by Lemma 6.10, $p_i(p_i - 1) \mid n - 1$ so $p_i \mid n - 1$ but $p_i \mid n$ and thus $p_i \mid 1$ ⊠
Therefore, $\nexists\, p$ s.t $p^2 \mid n$ i.e. n is square-free. □

Proposition 8.3. *No even Carmichael numbers exist.*

Proof. Carmichael numbers are square-free and composite so they have at least one odd prime factor. Let p be an odd prime and $p \mid n$ then by Korselt's Criterion, $p-1 \mid n-1$. However, $p-1$ is even so $n-1$ is even and thus n is odd.
Alternatively, if n is even then $n-1$ is odd so $(n-1)^{n-1} \equiv -1 \bmod n$
However, $n-1 \perp n$ so there exists an a coprime with n s.t. $n \not| \, a^{n-1}-1$

Lemma 8.4. *Let $n = ab$ then $a-1 \mid n-1 \iff a-1 \mid b-1$*

Proof. Let $a-1 \mid ab-1$, since $a-1 \mid (a-1)b$, we have that $a-1 \mid ab-1-(ab-b)$. Regrouping, $a-1 \mid b-1$.

Let $a-1 \mid b-1$ and therefore $a-1 \mid a(b-1)$. Since $a-1 \mid a-1$, $a-1 \mid ab-a+(a-1)$. Regrouping, $a-1 \mid ab-1$.

Proposition 8.5. *No Carmichael numbers with two prime factors exist.*

Proof. Let $n = pq$ where $p-1 \mid n-1$ and $q-1 \mid n-1$.
By Lemma 8.1, $p-1 \mid q-1$ and $q-1 \mid p-1$. Therefore, $p-1 = q-1 \implies p = q$ which contradicts the fact that Carmichael numbers are square-free.

Proposition 8.6. *$\forall a \in \mathbb{Z} : n \mid a^n - a$ and n is composite iff n is Carmichael.*

Proof. Let $n = p_1p_2 \dots p_k$ be a Carmichael number and therefore it is composite. Suppose $a \perp n$ then $n \mid a^{n-1}-1$ and therefore, $n \mid a^n - a$.
Otherwise, $\exists p_i \mid n$ s.t. $p_i \mid a$. For each prime factor p of n s.t. $p \not| \, a$, by Fermat, $p \mid a^{p-1}-1$ and by Korselt, $p \mid a^{n-1}-1$. Thus, $p \mid a^n - a$.
For each prime factor p' of n s.t. $p' \mid a$ we also have that $p' \mid a^n - a$.
Thus for every $p \mid n$, we have, $p \mid a^n - a$. By Lemma 2.10, $p_1p_2 \dots p_k = n \mid a^n - a$.

If $\forall a \in \mathbb{Z} : n \mid a^n - a$ then if $a \perp n$ by Lemma 2.12, $n \mid a^{n-1}-1$.
Since n is composite, n is Carmichael.

Proposition 8.7. $(6k+1)(12k+1)(18k+1)$ *is Carmichael if each factor is prime.*

Proof. Let $6k+1$, $12k+1$, $18k+1$ each be prime and let $n = (6k+1)(12k+1)(18k+1)$. We check that each factor minus one divides the product of the other two minus one:

- $(12k+1)(18k+1)-1 = 12 \cdot 18 \cdot k^2 + (12+18)k = 6k(36k+5)$ thus, $(6k+1)-1 \mid (12k+1)(18k+1)-1$
- $(6k+1)(18k+1)-1 = 6 \cdot 18 \cdot k^2 + (6+18)k = 12k(9k+2)$ thus, $(12k+1)-1 \mid (6k+1)(18k+1)-1$
- $(6k+1)(12k+1)-1 = 6 \cdot 12 \cdot k^2 + (6+12)k = 18k(4k+1)$ thus, $(6k+1)-1 \mid (12k+1)(18k+1)-1$

Thus for each prime p that divides n, by Lemma 8.1, $p-1 \mid n-1$. If each factor is prime then they are distinct so by Korselt's Criterion, n is Carmichael.
For example, $k = 1 \implies 7 \cdot 13 \cdot 19 = 1729$ is a Carmichael number. However, this formula does not produce all Carmichael numbers in particular it does not generate the first two Carmichael numbers: $3 \cdot 11 \cdot 17 = 561$ and $3 \cdot 13 \cdot 17 = 1105$

8.2 Mersenne Numbers

Proposition 8.8. *If $a^k - 1$ is prime then either $k = 1$ or $a = 2$*

Proof. $a \equiv 1 \bmod a - 1$ thus $a^k \equiv 1 \bmod a - 1$ so $a - 1 \mid a^k - 1$ if $a^k - 1$ is prime then either $a - 1 = a^k - 1$ i.e. $k = 1$ or $a - 1 = 1$ i.e. $a = 2$. □

Proposition 8.9. *If $2^k - 1$ is prime then k is prime*

Proof. Let $k = rt$. $2^r \equiv 1 \bmod 2^r - 1$ and thus $2^{rt} \equiv 1 \bmod 2^r - 1$ i.e. $2^r - 1 \mid 2^k - 1$. Because $2^k - 1$ is prime, either $2^r - 1 = 2^k - 1$ or $2^r - 1 = 1$ therefore, either $r = k$ or $r = 1$ thus $r \mid k \implies r = 1 \vee r = k$ i.e. k is prime.

Definition: $M_p = 2^p - 1$ is a Mersenne number if p is prime.

Proposition 8.10. *All prime divisors of M_p are of the form $q = 2pk + 1$*

Proof. Let $q \mid 2^p - 1$. $ord_q(2) \mid p$ so $ord_q(2) = 1$ or $ord_q(2) = p$. However, if $ord_q(2) = 1$ then $q \mid 2^1 - 1$ ⊠ Thus $ord_q(2) = p$. By Corollary 6.11, $ord_q(2) \mid q - 1$ thus $p \mid q - 1$ so $q = pr + 1$. Furthermore, since M_p is odd then q must also be odd. Thus, $q - 1$ is even so $2 \mid r$ and thus, $q = 2pk + 1$

Proposition 8.11. *If p is a prime of the form $4k - 1$ and $2p + 1$ is prime then $2p + 1 \mid M_p$ and therefore M_p is composite.*

Proof. Let $p = 4k - 1$ then $2p + 1 = 8k - 1$. Thus, by Propostion 7.10, $(2|p) = 1$. By Euler's Criterion, $2^{(2p+1-1)/2} = 2^p \equiv 1 \bmod 2p + 1$ thus $2p + 1 \mid 2^p - 1$.

Proposition 8.12. *If $q \mid M_p$ where q is an odd prime then $q \equiv \pm 1 \bmod 8$*

Proof. $2^p \equiv 1 \bmod q$ thus $2^{p+1} \equiv 2 \bmod q$ and because q is odd, $(2^{(p+1)/2})^2 \equiv 2 \bmod q$. Thus $(2|q) = 1$ so by Proposition 7.10, $q \equiv \pm 1 \bmod 8$.

Alternatively, by Proposition 8.10, $q = 2pk + 1$ thus $2^{(q-1)/2} = 2^{pk} \equiv 1 \bmod q$ thus by Euler's Criterion, $(2|q)$ so by Proposition 7.10, $q \equiv \pm 1 \bmod 8$.

Proposition 8.13. *If M_p is composite then it is a Fermat pseudoprime for base 2*

Proof. $2^p \equiv 1 \bmod M_p$ By Corollary 3.2, $p \mid 2^p - 2$ because p is prime, thus, $2^{2^p - 2} \equiv 1 \bmod M_p$ therefore, $2^{M_p - 1} \equiv 1 \bmod M_p$ and by hypothesis M_p is composite.

The first composite Mersenne number is $M_{11} = 23 \cdot 89$ and after that many Mersenne numbers are composite. In all, only 48 Mersenne primes are known as of 2015. However, Mersenne numbers are an efficient form to store large prime numbers and are especially useful for cryptography. Therefore, there has been significant research and computing power into finding Mersenne primes. In 2013, a distributed computing project known as The Great Internet Mersenne Prime Search proved that $M_{57,885,161}$ is prime making it the largest known prime number. It is an open question whether or not infinitely many Mersenne primes exist.

8.3 Fermat Numbers

Proposition 8.14. *If $a^n + 1$ is prime then $n = 2^k$ for some k.*

Proof. Suppose that $n = sr$ where s is odd. Then $a^r \equiv -1 \bmod a^s + 1$ so $a^s r \equiv (-1)^s \bmod a^r + 1$. Since a is odd, $(-1)^s = -1$ so $a^r + 1 \mid a^n + 1$. $a^n + 1$ is prime so $a^r + 1 = a^n + 1$ thus $s = 1$. The only odd factor of n is 1 therefore, $n = 2^k$

Definition: $F_k = 2^{2^k} + 1$ is the k^{th} Fermat Number.

Lemma 8.15. $F_{n+1} = F_0 \cdot F_1 \cdot \ldots \cdot F_n + 2$

Proof. For $n = 0$, $F_1 = 2^2 = 2^1 + 2$ Assume true for n.
Consider, $F_0 \cdot F_1 \cdot \ldots \cdot F_n \cdot F_{n+1} + 2 = (F_{n+1} - 2) \cdot F_{n+1} + 2 = (2^{2^{n+1}} - 1)(2^{2^{n+1}} + 1) + 2 = 2^{2 \cdot 2^{n+1}} + 1 = 2^{2^{n+2}} + 1$ by induction the result holds for all n.

Proposition 8.16. *For all i and j s.t. $i \neq k$, $F_i \perp F_j$*

Proof. Let $i > j$ then $F_i - F_0 \cdot F_1 \cdot \ldots \cdot F_{i-1} = 2$. Thus id $d \mid F_i$ and $d \mid F_j$ then $d \mid 2$. However, Fermat numbers are odd so $d = 1$.

Proposition 8.17. *If F_n is composite then it is a Fermat pseudoprime for base* 2

Proof. $2^{2^n} \equiv -1 \bmod F_n$ thus $(2^{2^n})^{2^{(2^n - n)}} \equiv (-1)^{2^{(2^n - n)}} \bmod F_n$ because $2^{(2^n - n)}$ is even, $2^{2^n \cdot 2^{(2^n - n)}} \equiv 1 \bmod F_n$ thus, $2^{2^{2^n}} \equiv 1 \bmod F_n$ Furthermore, $F_n = 2^{2^{2^n}}$ so $2^{F_n - 1} \equiv 1 \bmod F_n$ and by hypothesis F_n is composite.

Theorem 8.18 (Pepin's Test)**.** *F_k is prime iff $3^{(F_k - 1)/2} \equiv -1 \bmod F_k$ for $F_k > 3$.*

Proof. If $3^{(F_k - 1)/2} \equiv -1 \bmod F_k$ then $3^{F_k - 1} \equiv 1 \bmod F_k$ so $ord_{F_k}(3) \mid F_k - 1$ however, $ord_{F_k}(3) \nmid (F_k - 1)/2$ because $F_k - 1 = 2^{2^n}$ then $2^{2^n - 1} \nmid ord_{F_k}(3) \mid 2^{2^n}$, thus $ord_{F_k}(3) = F_k - 1 \leq \phi(F_k)$ thus by Corollary 6.4, F_k is prime.

If $F_k \neq 3$ is prime then by Quadratic Reciprocity, $(F_k|3)(3|F_k) = (-1)^{2^{2^{k-1}}} = 1$. Furthermore, $2 \equiv -1 \bmod 3$ so $F_k = 2^{2^k} + 1 \equiv 2 \equiv -1 \bmod 3$. However, $3 \not\equiv 1 \, mod \, 4$ so by Proposition 7.5, $(-1|3) = -1$ and thus $(F_k|3) = -1$ by Lemma 7.4. Because $(F_k|3)(3|F_k) = 1$ then $(3|F_k) = -1$, by Euler's Criterion, $3^{(F_k - 1)/2} \equiv -1 \bmod F_k$

□

After computing that $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ are all primes, Fermat conjectured that all Fermat numbers are prime. However, Euler proved that $641 \mid F_5$ and thus F_5 is composite.

Note: $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$.
Thus, $5^4 + 2^4 \equiv 0 \bmod 641$ so $2^{28} \cdot (5^4 + 2^4) \equiv 0 \bmod 641$
Write: $2^{28} \cdot (5^4 + 2^4) = 5^4 \cdot (2^7)^4 + 2^{32} = (5 \cdot 2^7)^4 + 2^{2^5}$ thus $(5 \cdot 2^7)^4 + 2^{2^5} \equiv 0 \bmod 641$.
However, $5 \cdot 2^7 \equiv -1 \bmod 641$ thus $(5 \cdot 2^7)^4 \equiv 1 \bmod 641$
therefore, $2^{2^5} + 1 \equiv 0 \bmod 641$

Using Pepin's and other primality tests, all Fermat numbers F_5 through F_{32} have been proven to be composite. It is unknown whether any other Fermat primes exist.

9 Primality Tests

Theorem 9.1 (Wilson's Theorem)**.** *$p \mid (p-1)! + 1$ iff p is prime.*

Proof. By Lemma 5.2, for each $a \in \Phi(p)$, there exists a unique $x \in \Phi(p)$ s.t. $ax \equiv 1 \bmod p$ because $a \perp p$. Now consider x, because $xa \equiv 1 \bmod p$ then a is the unique solution for x Suppose that $a^2 \equiv 1 mod p$ then $p \mid a^2 - 1$ so by Euclid's Lemma, $p \mid a-1$ or $p \mid p+1$ i.e. $a \equiv \pm 1 \bmod p$. Thus every element of $Phi(p)$ has a unique inverse distinct from itself except for 1 and $p-1$. Therefore, $(p-1)! \equiv 1 \cdot (p-1) mod p$ so $(p-1)! \equiv -1 \bmod p$ i.e. $p \mid (p-1)! + 1$.

Conversely, let $n = ab$ where $a < n$. Then $a \mid (n-1)!$ but if $n \mid (n-1)! + 1$ then $a \mid (n-1)! + 1$ so $a \mid (n-1)! + 1 - (n-1)!$ so $a \mid 1$. Thus, n is prime. ☐

Theorem 9.2 (Lucas's Test)**.** *If there exists an a s.t. $a^{n-1} \equiv 1 \bmod n$ and for every proper divisor m of $n-1$, $a^m \not\equiv 1 \, mod \, n$ then n is prime.*

Proof. Let $a^{n-1} \equiv 1 \bmod n$ thus, $ord_n(a) \mid n-1$. Assume that $ord_n(a) < n-1$. However, since $ord_n(a)$ is a divisor of m it is a proper divisor and therefore, $a^{ord_n(a)} \not\equiv 1 mod n$ but by definition the order satisfies this relation ⊠ The assumption is false, $ord_n(a) = n-1$ and thus, $n-1 \mid \phi(n)$ so by Corollary 6.4, n is prime. ☐

Theorem 9.3 (Proth's Theorem)**.** *Let $n = h \cdot 2^m + 1$ where $h < 2^m$ and $2 \not| h$. If p is an odd prime and $p^{(n-1)/2} \equiv -1 \bmod n$ then n is prime.*

Proof. Let $p^{(n-1)/2} \equiv -1 \bmod n$ and let q be a prime divisor of n i.e. $n = qc$. Because $q \mid n$ then $p^{(n-1)/2} \equiv -1 \bmod q$ so by Lemma 8.1, $p \perp q$. Because $p^{(n-1)/2} \equiv -1 \bmod q$ then $p^{n-1} \equiv 1 \bmod q$ therefore, $ord_q(p) \not| (n-1)/2$ and $ord_q(p) \mid n-1$ thus $h \cdot 2^{m-1} \not| ord_q(p) \mid h \cdot 2^m$ therefore, $2^m \mid ord_q(p)$. However, $ord_q(p) \mid q-1$ so $2^m \mid q-1$ Write $q - 1 = r \cdot 2^m$ for $r \geq 1$. Thus, $n - q = (h-r) \cdot 2^m$ so $2^m \mid n - q$ However, $n = qc$ so $n - q = q(c-1)$ so $2^m \mid q(c-1)$. q is odd so $q \perp 2^m$ so by Euclid's Lemma, $2^m \mid c-1$. Write $c - 1 = s \cdot 2^m$ thus $n = qc$ so $h \cdot 2^m + 1 = (r \cdot 2^m + 1)(s \cdot 2^m + 1)$. Simplifying, $h = rs \cdot 2^m + r + s$ but by hypothesis, $h < 2^m$ so $s = 0$ thus $c = 1$ therefore $n = q$ implying that n is prime. ☐

Lemma 9.4. *Let $p = d \cdot 2^s + 1$ where $2 \not| d$ be prime. Then for any a s.t. $p \not| a$, either $a^d \equiv 1 \bmod p$ or for some $0 \leq r \leq s-1$ it holds that $a^{d \cdot 2^r} \equiv -1 \bmod p$*

Proof. If $a \perp p$ then by Fermat's Little Theorem, $p \mid a^{p-1} - 1$. However, $a^{p-1} - 1 = (a^d)^{2^s} - 1$ factoring, $a^{p-1} - 1 = ((a^d)^{2^{s-1}} - 1)((a^d)^{2^{s-1}} + 1)$ factoring each difference of squares, $a^{p-1} - 1 = (a^d - 1)(a^d + 1)(a^{d \cdot 2} + 1)(a^{d \cdot 2^2} + 1) \cdots (a^{d \cdot 2^{s-1}} + 1)$ but $p \mid a^{p-1} - 1$ so by Euclid's Lemma p divides at least one factor.
Thus, $p \mid a^d - 1$ or for some $0 \leq r \leq s-1$, $p \mid a^{d \cdot 2^r} + 1$. ☐

Theorem 9.5 (Miller-Rabin Test)**.** *Let $n = d \cdot 2^s + 1$ where $2 \not| d$ and choose $a \perp n$. If $a^d \not\equiv 1 \, mod \, n$ and for every $0 \leq r \leq s-1$, $a^{d \cdot 2^r} \not\equiv -1 \, mod \, n$ then n is composite.*

Proof. The theorem follows from the contrapositive of Lemma 9.4. Numbers that fail the Miller-Rabin Test for a are known as strong probable primes for base a. ☐