1. Elementary number-theoretic notions

Definition. if $a = dq$ then $d|a$, i.e. d divides a.

Lemma 1. *If $d|a$ and $d|b$ then $d|\,(ax+by)$.*

Proof. $a = dk$ and $b = dk'$ then $s = ax + by = d\,(kx + k'y)$. $\square$

Definition. The **greatest common divisor** $\gcd(a,b)$ of two integers a,b is such that $\gcd(a,b)\,|a$ and $\gcd(a,b)\,|b$ and if d divides both a,b then $\gcd(a,b) \le d$.

Lemma 2. $\gcd(a,ka) = |a|$.

Proof. Clearly $\gcd(a,ka)$ divides both a and ka. No larger d could divide both since $\gcd(a,ka)$ is the largest d that divides a. $\square$

Theorem 3. *Division theorem. For any integer a and any positive integer n, there exist unique integers q,r such that $0 \le r < n$ and $a = qn + r$. $q = \lfloor a/n \rfloor$ is the **quotient** and $r = a \mod n$ is the **residue**.*

Theorem 4. $\gcd(a,b)$ is the smallest positive element of the set $\left\{s \middle| s = ax + by\,,\ (x,y) \in \mathbb{Z}\times\mathbb{Z}\right\}$.

Proof. Let $s = ax + by$, for some x,y, be the minimum element and $q = \lfloor a/s \rfloor$. Then by the division theorem

$$\begin{aligned} a \mod s &= a - qs \\ &= a - q\,(ax+by) \\ &= a\,(1-qx) + b\,(-qy) \end{aligned}$$

and hence $a \mod s$ is a linear combination of a,b. But $a \mod s < s$ and so $a \mod s = 0$. Similarly $b \mod s = 0$ and so $s|a$ and $s|b$ and by definition $\gcd(a,b) \ge s$. But $\gcd(a,b)\,|\,(ax+by) = s$ and so $\gcd(a,b) \le s$. So $\gcd(a,b) = s$. $\square$

Corollary 5. *If $d|a$ and $d|b$ then $d|\gcd(a,b)$.*

Proof. Since $\gcd(a,b)$ is linear a combination d divides it. $\square$

Corollary 6. $\gcd(na,nb) = n\gcd(a,b)$.

Proof. $\gcd(na,nb)$ is the smallest positive element of $\left\{s \middle| s = anx + bny\,,\ (x,y) \in \mathbb{Z}\times\mathbb{Z}\right\}$ which is n times the smallest element of $\left\{s \middle| s = ax + by\,,\ (x,y) \in \mathbb{Z}\times\mathbb{Z}\right\}$. $\square$

Corollary 7. *If $n|ab$ and $\gcd(a,n) = 1$, then $n|b$.*

Proof. Intuitively there's nothing else for n to divide. $1 = ax + ny$ and $ab = nk$ implies $b = abx + ny = n(kx + y)$. $\square$

Definition. If $\gcd(a,b) = 1$ then a,b are **relatively prime**.

Theorem 8. *If $\gcd(a,p) = \gcd(b,p) = 1$ then $\gcd(ab,p) = 1$.*

Proof. Since $ax + py = bx' + py' = 1$ we have that

$$ab\,(xx') + p\,(ybx' + y'ax + pyy') = 1$$

$\square$

Definition. Integers $n_1, n_2, \ldots, n_k$ are **pairwise relatively prime** if $\gcd(n_i,n_j) = 1$ for all $i \ne j$.

Theorem 9. *For all primes p and integers a, b if $p|ab$ then either $p|a$ or $p|b$ or both.*

Proof. Towards a contradiction suppose $p \nmid a$ and $p \nmid b$. Then $\gcd(a,p) = \gcd(b,p) = 1$ since the only divisors of p are p and 1. Then by above $\gcd(ab,p) = 1$, which contradicts $p|ab$ (which implies that $\gcd(ab,p) = p$). $\square$

Theorem. *Unique factorization. For any integer a*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

such that $p_1 < p_2 < \cdots < p_r$ and $e_i > 0$ is unique a factorization of a.

Definition. $[a]_n = \{a + kn : k \in \mathbb{Z}\}$ is the **equivalence class** or **residue class** of a module n. Equivalently $a \equiv b \pmod{n}$.

Definition. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \left\{[a]_n \,\middle|\, 0 \le a \le n-1\right\}$ is the cyclic group of order n.

1.1. **Exercises.**

Exercise 10. If $0 < b < a$ and $c = a + b$ the $c \mod a = b$.

Proof. $c \mod a = (a+b) \mod a = a \mod a + b \mod a = b$ since $b < a$. $\square$

Exercise 11. Infinitude of primes.

Proof. Pick your finite number of primes $p_1, p_2, \ldots, p_k$. Then $p = p_1 p_2 \cdots p_k + 1$ is not divisible by any of them. Why? For each p_i it's the case that $p = qp_i + 1$ and so $p - qp_i = 1$ and therefore $\gcd(p, p_i) = 1$. So either p is a prime distinct from p_i or p is composite but not divisible any of the p_i and hence has a prime factor distinct from any of the p_i. $\square$

Exercise 12. $|$ is transitive.

Proof. If $a|b$ then $b = ka$. If $b|c$ then $c = k'b$ and so $c = kk'a$. $\square$

Exercise 13. If p is prime and $0 < k < p$ then $\gcd(k,p) = 1$.

Proof. Ummm? Since p is prime (i.e. no factors) $\gcd(k,p)$ could only be p or 1. But simultaneouslygcd $(k,p) \le k < p$. Hence $\gcd(k,p) = 1$. $\square$

Exercise 14. If $0 < k < p$ then $p \middle| \binom{p}{k}$. Corollary $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Proof. I don't understand this?

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

so clearly $p \left| \binom{p}{k} \right.$ since $p|p!$??? I guess if p weren't smaller than one of the factors in the denominator could cancel the p but since p is prime that's not possible. Finally since

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

and so the only terms which aren't a multiple of p are $a^{p-0}b^0$ and $a^{p-p}b^p$. Hence

$$\begin{aligned} (a+b)^p \mod p &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \mod p \\ &= a^p + b^p \mod p \end{aligned}$$

□

Exercise 15. If $a, b > 0$ and $a|b$ then for any integer x $(x \mod b) \mod a = x \mod a$. Also $x \equiv y \pmod b$ implies $x \equiv y \pmod a$ for any integers x, y.

Proof. Firstly $a|b$ implies $b = ak$

$$\begin{aligned} x &= \lfloor x/b \rfloor b + x \mod b \\ &= (k \lfloor x/b \rfloor) a + x \mod b \end{aligned}$$

So $x \mod b = x - (k\lfloor x/b \rfloor) a$. Then

$$(x - (k \lfloor x/b \rfloor) a) \mod a = x \mod a$$

If $x \equiv y \pmod b$ then $x - y \equiv 0 \pmod b$ which implies $x - y = qb$, but then $x - y = qka$ and so $x \equiv y \pmod b$. □

Exercise 16. Show how to determine whether a given β-bit integer n is a nontrivial power of some number in time polynomial in β.

Note that $a \geq 2$ since $1^k = 1$ for all k. Also note that n is a nontrivial power than k is at most $\lfloor \log n \rfloor$ since $a^{\lfloor \log n \rfloor + 1} > n$ for all $a \geq 2$. To determine if n is a nontrivial power compute all $\lfloor \log n \rfloor = O(\beta)$ roots using binary search, which can be run in $O(\beta)$ time, and hence totally in time $O(\beta^2)$.

Use binary search we guess an initial value of for the mth root $a = 2^{\lfloor \log n \rfloor / m}$ (i.e. we guess that n is a power of 2). If $a^m = n$ then we're done. Otherwise we bisect depending on $a^m > n$ or $a^m < n$. This will end after $\lfloor \log n \rfloor$ iterations.

Exercise 17. Show that gcd is associative, i.e.

$$\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$$

Proof. First

$$\begin{aligned} \gcd(a, \gcd(b, c)) &= ax + \gcd(b, c)\, y \\ &= ax + (bx' + cy')\, y \\ \gcd(\gcd(a, b), c) &= \gcd(b, c)\, x'' + cy'' \\ &= (bx''' + y''')\, x'' + cy'' \end{aligned}$$

By minimality they're equal. □

Prove unique factorization.

Proof. Existence: assume it's from all numbers 1 to $n - 1$. If n is prime then we're done. Otherwise $n = ab$ where $a < n$ and $b < n$ with $a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ and $b = q_1^{f_1} q_2^{f_2} \cdots q_n^{f_n}$ and so $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} q_1^{f_1} q_2^{f_2} \cdots q_n^{f_n}$. Uniqueness: suppose

$$a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

and

$$a = q_1^{f_1} q_2^{f_2} \cdots q_n^{f_n}$$

Then

$$\frac{a}{p_1^{e_1}} = p_2^{e_2} \cdots p_m^{e_m}$$

So $p_1^{e_1}\Big| a$. By Euclid's lemma[1] $p_1^{e_1}$ divides one $q_i^{f_i}$. Relable such that $p_1^{e_1}$ divides one $q_1^{f_1}$. But $q_1^{f_1}$ is a power of a prime and only powers of q_1 divide it. Therefore $p_1 = q_1$. Reasoning the same way

$$\frac{a}{p_1^{e_1} p_2^{e_2}} = p_3^{e_3} \cdots p_m^{e_m}$$

and on we get that $p_i = q_i$. This shows that $m \leq n$ and $p_i = q_i$ for all $i \leq m$. Reasoning in reverse shows that the same for $n \leq m$. □

2. Greatest Common Divisor

Theorem 18. *GCD Recursion.*

For any nonnegative integer a and any positive integer b such that $b < |a|$

$$\gcd(a, b) = \gcd(a \mod b, b)$$

To understand this intuitively think about a divisor of a and b as a way of cutting up both (same size cuts) so that after some number of cuts (different for each) none of either is left. Suppose $k = \gcd(a, b)$. Then for some q it's the case that $a = qk$. Similarly $b = rk$, with $r < q$. Now $a - b = (q - r)k$ but still a multiple of k (duh any divisor divides any linear combination of a, b). But if $r \ll q$ then we could write $a - mb = (q - mr)k$ for some m. So $a \mod b$ is just $a - mb$ for largest m such that $q - mr > 0$.

The Extended Euclid's algorithm code works because if $d = \gcd(a, b) = ax + by$ then

$$\begin{aligned} d &= \gcd(a, b) \\ &= ax + by \\ &= \gcd(b, a \mod b) \\ &= bx' + (a \mod b)\, y' \\ &= bx' + (a - b\lfloor a/b \rfloor)\, y' \\ &= ay' + b\,(x' - \lfloor a/b \rfloor y') \end{aligned}$$

and so for the equality to hold it has to be the case that $x = y'$ and $y = x' - \lfloor a/b \rfloor y'$.

For Iterative Extended Euclid let

$$\begin{aligned} x_0, x_1 &= 1, 0 \\ y_0, y_1 &= 0, 1 \end{aligned}$$

and $r_0 = a, r_1 = b, r_i = a_i \mod b_i$. Note that

$$\begin{aligned} a &= q_1 b + r_2 \\ r_2 &= a - qb \\ b &= q_2 r_2 + r_3 \\ r_3 &= b - q_2 r_2 \end{aligned}$$

[1] If $p|ab$ then $p|a$ or $p|b$.

So

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i \\ &\Longleftrightarrow \\ a_{i+1} \mod b_{i+1} &= a_{i-1} \mod b_{i-1} - \left\lfloor \frac{a_i}{b_i} \right\rfloor \cdot (a_i \mod b_i) \end{aligned}$$

Then

$$\begin{aligned} ax_0 + by_0 &= a = r_0 \\ ax_1 + bx_1 &= b = r_1 \end{aligned}$$

So $ax_0 + by_0 = \gcd(a, b)$ for the base case(s). Then by induction

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i \\ &= (ax_{i-1} + by_{i-1}) - q_i (ax_i + by_i) \\ &= (ax_{i-1} - aq_i x_i) + (by_{i-1} - bq_i y_i) \\ &= a (x_{i-1} - q_i x_i) + b (y_{i-1} - q_i y_i) \end{aligned}$$

So letting $x_{i+1} = x_{i-1} - q_i x_i$ and $y_{i+1} = y_{i-1} - q_i y_i$ we get that when the algorithm terminates at step k

$$\gcd(a, b) = r_k = a (x_{k-1} - q_k x_k) + b (y_{k-1} - q_k y_k)$$

Exercise 19. Prove $a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_m^{f_m}$ implies

$$\gcd(a, b) = p_1^{e_1 \wedge f_1} p_2^{e_2 \wedge f_2} \cdots p_n^{e_m \wedge f_m}$$

Proof. Well duh? Suppose for some of j it's the case that $e_j < q_j < f_j$ and $p_j^{q_j}$ is a factor of $\gcd(a, b)$. Well clearly for whichever of a, b q_j is greater power than p_j's power in a, b won't be divisible by $\gcd(a, b)$. □

Prove that for all integers a, b, k

$$\gcd(a, b) = \gcd(a + kb, b)$$

Proof. Duh. $a + kb \mod b = a \mod b$ so

$$\gcd(a + kb, b) = \gcd(a \mod b, b) = \gcd(a, b)$$

□

Show how to find integers $x_0, x_1, \ldots, x_n$ such that

$$\gcd(a_0, a_1, \ldots, a_n) = a_0 x_0 + \cdots + a_0 x_n$$

Proof. By way of example:

$$\begin{aligned} \gcd(32, 20) &= 4 = 2 \cdot 32 - 3 \cdot 20 \\ \gcd(10, 4) &= 2 = 10 - 2 \cdot 4 = 10 - 2 \cdot (2 \cdot 32 - 3 \cdot 20) \\ &= 10 - 4 \cdot 32 + 6 \cdot 20 \end{aligned}$$

□

3. Groups

Definition 20. A *group* $G = (S, \oplus)$ is a set with a binary operation such that

(1) For $a, b \in S$ it's the case that $a \oplus b \in S$.
(2) There exists an identity e such that $e \oplus a = a \oplus e = a$ for all $a \in S$.
(3) $\oplus$ is associative.
(4) There exist inverses, i.e. for all a there exists b such that $a \oplus b = b \oplus a = e$. Typically written as $-a$ or a^{-1}.

If the operation is commutative then the group is called an *abelian* group. If $|S| < \infty$ then the group is a *finite* group.

Example 21. $(\mathbb{Z}_n, +)$ is the integers modulo n with addition modulo n as the operation.

Example 22. $(\mathbb{Z}_n^*, \times)$ is the integers modulo n which are also co-prime to n (so that each one has a unique inverse [gcd]) with multiplication modulo n as the operation. $\mathbb{Z}_n^*$ is well-defined since $a \equiv a + kn \mod n$ and by exercise something $\gcd(a, n) = 1$ implies $\gcd(a + kn, n) = 1$. Since $[a]_n = \{a + kn \, : \, k \in \mathbb{Z}\}$, $\mathbb{Z}_n^*$ is well-defined.

Example 23. You can use ExtendedGCD to compute inverses. Suppose $\mathbb{Z}_{11}^*$ and we want the inverse of 5. Then $\text{ExtendedGCD}(5, 11) = 1 = 5 \cdot (-2) + 11 \cdot 1$ so $5 \cdot 2 \mod 11 = 1$.

$\phi(n)$ is Euler's phi function and it counts the number or numbers less than n and co-prime to n. Analytically for p prime

$$\phi(n) = n \left(\prod_{p|n} \left(1 - \frac{1}{p} \right) \right)$$

Why does this work? Take for example 45 with prime factors 3 and 5. How many multiples of 3 are there in $0, 1, \ldots, 45 - 1$? Well $45/3 = 15$ duh. Therefore

$$45 \left(1 - \frac{1}{3} \right) = 45 - \frac{45}{3} = 30$$

are not divisble by 3. How many of the rest are divisible by 5? Those are just the numbers in $0, 1, \ldots, 44$ divisible by 5 but not divisible by 15 (because those have already been taken out) i.e.

$$30 - \frac{45}{5} + \frac{45}{15} = 30 - 9 + 3 = 24$$

But

$$\begin{aligned}
45 \left(1 - \frac{1}{3} \right) - \frac{45}{5} + \frac{45}{15} &= 45 \left(1 - \frac{1}{3} \right) - \frac{45}{5} + \frac{45}{15} \\
&= 45 \left(\left(\frac{15}{15} - \frac{5}{15} \right) - \frac{3}{15} + \frac{1}{15} \right) \\
&= 45 \left(\frac{8}{15} \right) \\
&= 45 \left(\frac{2}{3} \right) \left(\frac{4}{5} \right) \\
&= 45 \left(1 - \frac{1}{3} \right) \left(1 - \frac{1}{5} \right)
\end{aligned}$$

Another way to look at it is to expand $45\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$$45\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=45\left(1-\frac{1}{3}-\frac{1}{5}+\frac{1}{15}\right)$$

The first subtraction removes multiples of 3, the second removes multiples of 5, the addition puts back double counts. Inductively generalizing is clear.

Definition 24. A subset $S' \subset S$ is a *subgroup* if S' is also a group.

Theorem 25. *If $S' \subset S$ of a finite group. is nonempty and closed then S' is a subgroup.*

Proof. Associativity of the operation on S' is inherited from associativity of the operation on S. Remains to prove identity and inverses. Since S is nonempty take $x \in S$ and add it to itself over and over again, i.e. compute nx for $n \in \mathbb{N}$. Eventually there will be a repeat (otherwise S' would have cardinality equal to $\mathbb{N}$). Let m, m' be distinct such that $mx = m'x$. Then $|m - m'|\, x = 0 \in S$. Then to prove inverses compute nx until $n'x = 0$. Then $x + (n' - 1)\, x = 0$ and so $(n' - 1)\, x$ is the inverse of x. □

Lagrange's theorem: the order of a subgroup divides the order of the group

Proof. Cosets equivalence relation partition the set. □

Corollary 26. *If $S' < S$ then $|S'| \leq |S|/2$.*

Proof. 2 is the smallest divisor. □

Definition 27. The subgroup generated by an element a is $\langle a\rangle = \left\{a^k \,:\, k \geq 1\right\}$.

Definition 28. The order of the subgroup is the minimal t such that $a^t = 1$.

Theorem 29. *The order of an element a is equal to the order of $\langle a\rangle$.*

Corollary 30. $a^1, a^2, \ldots$ *is periodic with period $t = ord\,(a)$.*

Corollary 31. $a^{|S|} = e$

Proof. By Lagrange's theorem the order of $\langle a\rangle$ divides $|S|$. □

Exercise 32. If p is prime and $e > 0$ then

$$\phi\left(p^e\right) = p^{e-1}\,(p-1)$$

Proof. Duh

$$p^{e-1}\,(p-1) = p^e - p^{e-1} = p^e\left(1-\frac{1}{p}\right)$$

□

Show that for any $n > 1$ and $a \in \mathbb{Z}_n^*$, $f_a(x) = ax \mod n$ is a permutation of $\mathbb{Z}_n^*$.

Proof. Coset map. Hinges on inverses. □

4. Solving modular linear equations

The equation $ax \equiv b \mod n$ has a solution iff $b \in \langle a \rangle$.

Theorem 33. *For positive integers a, n if $d = \gcd(a, n)$ then*

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d) - 1)\, d\}$$

Proof. Firsly $\langle d \rangle \subset \langle a \rangle$: by Euclid's algorithm

$$ax + ny = d = \gcd(a, n)$$

so $ax \equiv d \mod n$ $(d < n)$. So $d \in \langle a \rangle$ and hence $\langle d \rangle \subset \langle a \rangle$.

Now for $\langle a \rangle \subset \langle d \rangle$: if $m \in \langle a \rangle$ then $m = ax + ny$ but $d|a$ and $d|n$ so $d|m$ and hence $m \in \langle d \rangle$. Note that this means $|\langle a \rangle| = |\langle d \rangle| = n/d$ since there are n/d d-sized blocks in $0, \ldots, n-1$. □

Corollary 34. *$ax \equiv b \mod n$ is solvable iff $d|b$.*

Proof. $ax \equiv b \mod n$ has a solution iff $[b] \in \langle a \rangle$ i.e. $b \mod n \in \langle a \rangle = \{0, d, 2d, \ldots, ((n/d) - 1)\, d\}$ there if $0 < b < n$ then $b \in \langle a \rangle$ iff $d|b$. If $b < 0$ or $b \geq n$ then just find b' such that $b \in [b']$ and $0 < b' < n$. □

$ax \equiv b \mod n$ either has d distinct solutions (for x) or none.

Proof. If $ax \equiv b \mod n$ then $b \in \langle a \rangle$. Since $|a| = |\langle a \rangle|$ the sequence $ai \mod n$ is periodic with period $|\langle a \rangle| = n/d$. If $b \in \langle a \rangle$ then b appears exactly d times in the sequence $ai \mod n$ since each value of ai repeats d times in the d length n/d blocks from 0 to $n-1$. The locations of the repeats of b in $0, 1 \ldots, n-1$ are the xs. □

Summary: $ax \equiv b \mod n$ if $b \in \langle a \rangle$,$\langle a \rangle = \langle d \rangle$, so $ax \equiv b \mod n$ has a solution iff $dx \equiv b \mod n$ has solution, which has a solution iff $d|b$.

Corollary 35. *If $ax \equiv b \mod n$ has a solution then*

$$x_0 = x' \left(\frac{b}{d} \right) \mod n$$

where $\gcd(a, b) = d = ax' + ny'$ is a solution.

Proof. Firsly $d|b$ so b/d is an integer. Then $ax_0 \equiv ax' \left(\frac{b}{d} \right) (\mod n)$ and since $ax' = d - ny'$ it's the case that $ax' \equiv d \mod n$ so

$$\begin{aligned} ax_0 &\equiv d \left(\frac{b}{d} \right) (\mod n) \\ &\equiv b (\mod n) \end{aligned}$$

□

Theorem 36. *Suppose x_0 is a solution for $ax \equiv b \mod n$. Then $x_i = x_0 + i \left(\frac{n}{d} \right)$ for $i = 0, 1, \ldots, d-1$ are all solutions.*

Just remember that $\langle a \rangle$ repeats every n/d blocks.

Proof. Since $n/d > 0$ and $0 \leq i\,(n/d) < n$ the values $x_0, x_1, \ldots, x_{d-1}$ are all distinct mod$n$. Then since x_0 is a known solution $ax_0 \equiv b \mod n$ and so since $d|a$ and $d|n$

$$\begin{aligned} ax_i &= a\,(x_0 + i\,(n/d))\,(\mod n) \\ &= ax_0 + ai\,(n/d)\,(\mod n) \\ &= ax_0\,(\mod n) \\ &= b \end{aligned}$$

□

If $d|b$ then

$$b = \frac{b}{d}d = ax'\left(\frac{b}{d}\right) + ny'\left(\frac{b}{d}\right)$$

and so

$$\begin{aligned} b &\equiv a\left(x'\left(\frac{b}{d}\right)\right) + ny'\left(\frac{b}{d}\right) \mod n \\ &\equiv a\left(x'\left(\frac{b}{d}\right)\right) \mod n \end{aligned}$$

This naturally suggests an algorithm for solving modular equations

Algorithm 1 Moduler equations

```
ModularEqnSolver(a,b,n)
(d, x', y') = ExtendedGCD(a,n)
if d|b
    x_0 = x' b/d ( mod n)
    for i = 0 to d - 1
        print (x_0 + i n/d) mod n
else
    print "no solutions"
```

Corollary 37. *For $n > 1$ if $\gcd(a, n) = 1$ then $ax \equiv b \mod n$ has a unique solution modulo n.*

Proof. $ax \equiv b$ has d distinct solutions (if any) where $d = \gcd(a, n)$. □

Corollary 38. *For $n > 1$, if $\gcd(a, n) = 1$ then $ax \equiv 1 \mod n$ has a unique solution modulo n. Otherwise it has no solutions.*

Proof. If $\gcd(a, n) = 1$ then $1 = ax' + ny'$ and so $ax' \equiv 1 \mod n$. Assume $d \neq 1$. Then $ax \equiv 1 \mod n$ has no solutions because $d|1$ implies $d = 1$. □

Exercise 39. If $\gcd(a, n) = 1$ then $ax \equiv ay \mod n$ implies $x \equiv y \mod n$. Show that $\gcd(a, n) = 1$ is necessary by producing a counter example.

Proof. You can cancel whenever the common factor has an inverse. Since $\gcd(a, n) = 1$ a has a multiplicative inverse. Therefore you can cancel. □

Exercise 40. Consider $f(x) = f_0 + f_1 x + \cdots + f_t x^t \pmod{p}$ with $f_i \in \mathbb{Z}_p$. Prove that if $f(a) = 0$ then $f(x) \equiv (x-a)\, g(x) \pmod{p}$ for some $g(x)$ of degree $t-1$. Prove by induction that f can have at most t distinct zeros module p.

The lemma in the exercise concerns whether Euclidean division by $(x-a)$ is possible. Suppose $f(x) = 2x^2 + x + 1$. Then

$$r(x) = f(x) - \frac{2}{1} x^{2-1}(x-a) = 2x^2 + x + 1 - 2x(x-a) = x + 2xa + 1 = x(2a+1) + 1$$

So $\deg(f_1) = \deg(f) - 1$ and we get that

$$\begin{aligned} f(x) &= g(x)(x-a) + r(x) = 2x(x-a) + x(2a+1) + 1 \\ &= 2x^2 - 2ax + 2ax + x + 1 = 2x^2 + x + 1 \end{aligned}$$

When does this work in general? Meaning for arbitrary $h(x)$? Well it works whenever you can cancel the highest order term in $f(x)$, because you're essentially reducing the order of $f(x)$ (and to do that you just need to cancel the highest order term). Let $f(x) = f_0 + f_1 x + \cdots + f_n x^n$ and $h(x) = h_0 + h_1 x + \cdots + h_m x^m$. Note that if $n = 0$ or $m > n$ then the result is trivial. Otherwise we need to be able to write

$$r(x) = f(x) - \frac{f_n}{h_m} x^{n-m} h(x)$$

So what do we need for this? We need the coefficients of f and h to come from at least commutative rings[2] but we also need to be able to divide f_n by h_m so the ground set should be a field. If $h(x)$ is monic though all need is that the polynomials are over a commutative ring.

Lemma 41. *Let R be a commutative ring and let $f(x)$ be a polynomial with coefficients in R, of degree $n \geq 0$. If $h(x)$ is a monic polynomial with coefficients in R, then there exist polynomials $g(x)$ and $r(x)$, with the degree of r less than the degree of f such that*

$$f(x) = g(x)\, h(x) + r(x)$$

Proof. If degree of f is zero then there's nothing to prove: either degree of h is 0, in which case $h(x) = 1$ (since monic), or it has a higher degree in which case we take $g(x) = 0$ and $r(x) = f(x)$. Therefore assume the base case and let $n = \deg(f) > 0$. If $m = \deg(h) > n$ then do the same thing as before: take $g(x) = 0$ and $r(x) = f(x)$. So assume $n \geq m > 0$. Then if $f(x) = f_0 + f_1 x + \cdots + f_n x^n$

$$f_1(x) = f(x) - f_n x^{n-m} h(x)$$

has degree less than n and so, by the induction hypothesis, $f_1(x) = g_1(x)\, h(x) + r(x)$ and hence

$$f(x) = \left(g_1(x) + f_n x^{n-m}\right) h(x) + r(x)$$

$\square$

Then for our case where $h(x) = x - a$ we have

$$f(x) = g(x)(x-a) + r(x)$$

Since $r(x)$ must be a constant (why?) and must be $f(a)$ since $f(a) = g(a) \cdot 0 + r(a)$. Finally if $f(a) \equiv_p 0$ then

$$f(x) = (x-a)\, g(x)$$

[2] I guess polynomial rings are always over at least commutative rings?

Suppse a' is another distinct root, i.e. $f(a') \equiv_p 0$ and $a \not\equiv_p a'$. So

$$f(a') = (a' - a)\, g(a')$$

Then since $a \not\equiv_p a'$ implies that $a - a' \not\equiv_p 0$ we know that $g(a') \equiv_p 0$ since $\gcd(a, n) = 1$ and $n|ab$ implies that $n|b$. Then we can repeat the process for with further roots $a'', a''', \ldots$.

5. Chinese Remainder Theorem

Definition 42. Direct product $A \times B$ of two rings A and B is simply the ring over the tuples $\left\{(a, b) \,\middle|\, a \in A, b \in B\right\}$ with the operations defined coordinate-wise.

How do you solve the system of equations

$$\begin{aligned} x &\equiv_3 2 \\ x &\equiv_5 3 \\ x &\equiv_7 2 \end{aligned}$$

The chinese remainder theorem

Theorem 43. *If* $n = p_1^{r_1} \cdots p_k^{r_k}$ *and* $\gcd(p_i, p_j) = 1$ *then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

where $\times$ *is direct product.*

Proof. We need to demonstrate the isomorphism. Suppose $a \in \mathbb{Z}_n$, then $(a \mod p_1^{r_1}, \ldots, a \mod p_k^{r_k})$. For the reverse direction suppose we have $(a_1 \mod p_1^{r_1}, \ldots, a_k \mod p_k^{r_k})$. We need a way to manufacture an a such that

$$\begin{aligned} a \mod p_1^{r_1} &= a_1 \\ &\vdots \\ a \mod p_k^{r_k} &= a_k \end{aligned}$$

Towards this end let $m_i = n/p_i^{r_i}$ and $c_i = m_i \left(m_i^{-1} \mod p_i^{r_i}\right)$. Since m_i and $p_i^{r_i}$ are coprime m_i^{-1} exists[3]. The c_i function as "basis vectors" since $c_i \mod p_j^{r_j} = 0$ and $c_i \mod p_i^{r_i} = \left(m_i \left(m_i^{-1} \mod p_i^{r_i}\right)\right) \mod p_i^{r_i} = \left(m_i m_i^{-1}\right) \mod p_i^{r_i} \mod p_i^{r_i} = 1$. Then

$$a = \sum_{i=1}^{k} a_i c_i$$

and the preceding arguments show that a satisfies the modular equations. So the mapping is a bijection. To see that it's a homomorphism note that since $p_i^{r_i}|n$ it's the case that $(x \mod n) \mod p_i^{r_i} = x \mod p_i^{r_i}$, then let $d = a + b$ and then

$$(a+b) \mod n = d \mod n \iff d_i \mod p_i^{r_i} = ((a_i + b_i) \mod n) \mod p_i^{r_i} = (a_i + b_i) \mod p_i^{r_i}$$

and similarly for $ab \mod n$. □

[3] Use ExtendedGCD to compute $\gcd\left(m_i, p_i^{r_i}\right)$.

Corollary 44. *If* $n = p_1^{r_1} \cdots p_k^{r_k}$ *and* $\gcd(p_i, p_j) = 1$ *then*

$$\begin{aligned} x &\equiv_{p_1^{r_1}} a_1 \\ &\vdots \\ x &\equiv_{p_k^{r_k}} a_k \end{aligned}$$

has a unique solution x *modulo* n.

Proof. Duh

$$x = \sum_{i=1}^{k} a_i c_i$$

□

If $n = p_1^{r_1} \cdots p_k^{r_k}$ *and* $\gcd(p_i, p_j) = 1$ *then*

$$\begin{aligned} x &\equiv_{p_1^{r_1}} a \\ &\vdots \\ x &\equiv_{p_k^{r_k}} a \end{aligned}$$

if and only if $x \equiv_n a$.

Proof. Let

$$\begin{aligned} x &\equiv_{p_1^{r_1}} a \\ &\vdots \\ x &\equiv_{p_k^{r_k}} a \end{aligned}$$

i.e. x solves all of the linear congruence relations. One such solution is obviously $x = a$. Any other solution x' is congruent to a modulo $p_1^{r_1} \cdots p_k^{r_k}$, i.e. $x' \equiv_n a \mod n$. Why? Because n is the lcm of all of the $p_i^{r_i}$ so it "rotates" all of the solutions around the right number of times. On the other hand if $x \equiv_n a$ then

$$x \mod p_i^{r_i} = (x \mod n) \mod p_i^{r_i} = (a \mod n) \mod p_i^{r_i} = a \mod p_i^{r_i}$$

□

Exercise 45. Prove that if $\gcd(a, n) = 1$ then

$$a^{-1} \mod n \leftrightarrow \left(a_1^{-1} \mod p_1^{r_1}, \ldots, a_k^{-1} \mod p_k^{r_k}\right)$$

Proof. By Chinese Remainder Theorem if a is unit, i.e. $\gcd(a, n) = 1$ then

$$1 \mod n = aa^{-1} \mod n \leftrightarrow \left(a_1 a_1^{-1} \mod p_i^{r_i}, \ldots, a_k a_k^{-1} \mod p_k^{r_k}\right) = (1, \ldots, 1)$$

□

Exercise 46. The number of x such that $f(x) \equiv_n 0$ equals the product of the number of x of each $f(x) \equiv_{p_i^{r_i}} 0$.

Proof. By the corollary to the Chinese Remainder theorem $f(x) \equiv_n 0$ if $f(x) \equiv_{p_i^{r_i}} 0$ for all i. If each $f(x) \equiv_{p_i^{r_i}} 0$ has r_i roots then there are $\prod_{i=1}^{k} r_i$ ways for all components of $(f_1, \ldots, f_n)$ to be 0. □

6. Powers

Recall that $\mathbb{Z}_n^*$ is group where the operation is multiplication module n and the elements x are such that $\gcd(x,n)=1$.

Theorem 47. ***Euler's theorem***. *For any integer $n>1$ and $a \in \mathbb{Z}_n^*$*

$$a^{\phi(n)} \equiv_n 1$$

Proof. By Langrange's theorem $|\langle a\rangle| \, | \, (|\mathbb{Z}_n^*| = \phi(n))$ and so

$$a^{\phi(n)\cdot|\langle a\rangle|} = \left(a^{|\langle a\rangle|}\right)^{\phi(n)} = 1^{\phi(n)}$$

$\square$

Lagrange's theorem. *If p is prime, then for all $a \in \mathbb{Z}_p^*$*

$$a^{p-1} \equiv_p 1$$

Proof. By Euler's and since for prime p it's the case that $\phi(p) = p-1$. $\square$

Corollary 48. *For all $a \in \mathbb{Z}_p$, we have $a^p \equiv_p a$.*

Definition 49. An element a **generates** $\mathbb{Z}_n^*$ if $|\langle a\rangle| = |\mathbb{Z}_n^*|$, i.e. every element of is a power of a.

Definition 50. A group $\mathbb{Z}_n^*$ is **cyclic** there exists $a \in \mathbb{Z}_n^*$ such that a generates $\mathbb{Z}_n^*$.

Theorem 51. *$\mathbb{Z}_n^*$ is cyclic for $2, 4, p^e, 2p^e$ for prime p and positive integer e.*

Definition 52. If a generates $\mathbb{Z}_n^*$ then the **discrete logarthim** of $e \in \mathbb{Z}_n^*$ is minimum z such that $a^z \equiv_p e$.

Theorem 53. *Discrete logarithm theorem. If $|\langle a\rangle| = \mathbb{Z}_n^*$ then $a^x \equiv_n a^y$ iff $x \equiv_{\phi(n)} y$.*

Proof. Suppose $x \equiv_{\phi(n)} y$. Then $x = y + k\phi(n)$ for some k. Then by Euler's theorem

$$\begin{aligned} a^x &\equiv_n a^{y+k\phi(n)} \\ a^x &\equiv_n a^y a^{k\phi(n)} \\ a^x &\equiv_n a^y \end{aligned}$$

Suppose $a^x \equiv_n a^y$. Since a generates $\mathbb{Z}_n^*$ it's the case that $|\langle a\rangle| = \phi(n)$. Therefore the sequence of powers of a is periodic with period $\phi(n)$. This is equivalent to $a^x \equiv_n a^y$ iff x and y are some number of periods apart, i.e. $x \equiv_{\phi(n)} y$. $\square$

Now on to roots of 1 modulo a prime power.

Theorem 54. *If p is an odd prime and $e \geq 1$, then*

$$x^2 \equiv_{p^e} 1$$

only has solutions $x = \pm 1$.

Proof. $x^2 \equiv_{p^e} 1$ is equivalent to $(x+1)(x-1) \equiv_{p^e} 0$ which is equivalent to $p^e | (x-1)(x+1)$. Since $p > 2$ it's the case that p divides either $x-1$ or $x+1$ but not both (otherwise p would divide $(x-1)-(x+1) = 2$). If $p \nmid (x-1)$, then $\gcd(p^e, x-1) = 1$ and so $p^e | (x+1)$, i.e. $x \equiv_{p^e} -1$. The symmetric argument is the same. $\square$

Definition 55. x is a **nontrivial** square root of 1, modulo n, if $x^2 \equiv_n 1$ and $x \neq -1 \neq 1$.

Corollary 56. *If there exists a nontrivial square root of 1, modulo n, then n is composite.*

Proof. By contrapositive of the previous theorem, if there exists a nontrivial root then n cannot be an odd prime or power of an odd prime. $\square$

Exercise 57. Given $\phi(n)$, how to compute $a^{-1} \mod n$ for $a \in \mathbb{Z}_n^*$ using Modular-Exponentiation.

Easy: compute $a^{\phi(n)-1}$ and then $a^{\phi(n)-1}a = a^{\phi(n)} = 1 \mod n$.

How does exponentiation by repeated squaring work? Take for example 3^8:

$$\left(\left(\left(3^2\right)^2\right)^2\right)^2 = 3^8$$

How about 3^7? The trick is to divide only even exponents: 3^7 doesn't divide "evenly" but 3^6 does. Then 3^3 again doesn't divide evenly but 3^2 does. So what should you do? Go in reverse order

$$3 \cdot \left(\left(3 \cdot 3^2\right)^2\right) = 3 \cdot \left(\left(3^3\right)^2\right) = 3 \cdot \left(3^6\right) = 3^7$$

How about another example: 3^{19}

$$\begin{aligned} 3 \cdot 3^{18} &\rightarrow 3^{18} \\ 3^{18} = \left(3^9\right)\left(3^9\right) &\rightarrow 3^9 \\ 3 \cdot 3^8 &\rightarrow 3^8 \\ 3^8 = \left(3^4\right)\left(3^4\right) &\rightarrow 3^4 \\ 3^4 = \left(3^2\right)\left(3^2\right) &\rightarrow 3^2 \\ 3^2 = 3 \cdot 3 &\rightarrow 3^1 \\ 3^1 = 3 \cdot 1 &\rightarrow 1 \end{aligned}$$

Do you see the pattern? The binary representation of 19 is 10011, which matches the order in which we took the square root or factored out a 3 and then took the square root. Why?

$$3^{19} = 3^{\left(1\cdot 2^0+1\cdot 2^1+0\cdot 2^2+0\cdot 2^3+1\cdot 2^4\right)}$$

You can think of exponentiation by repeated squaring as building up the exponent using shift and add: every squaring is a shift and every multiplication by the base is adding 1. For example: first shift in one 3

$$(3 \cdot 1) = 3^{0b1}$$

Then shifting left twice

$$\left(\left(3^{0b1}\right)^2\right)^2 = \left(3^{2\times 0b1}\right)^2 = \left(3^{0b10}\right)^2 = 3^{2\times 0b10} = 3^{0b100}$$

Then shift left again and add 1

$$3 \cdot \left(3^{0b100}\right)^2 = \left(3^{0b1000+0b0001}\right) = 3^{0b1001}$$

and again

$$3 \cdot \left(3^{0b1001}\right)^2 = 3^{0b10011} = 3^{19}$$

7. RSA

7.1. **Public-key cryptosystems.** Let P_A and S_A be the public key and secret keys of agent A respectively. The **keys specify bijections** from the message space $\mathcal{D}$ that are mutual inverses, i.e. $P_A : \mathcal{D} \to \mathcal{D}$ and $S_A : \mathcal{D} \to \mathcal{D}$ and for $M \in \mathcal{D}$

$$\begin{aligned} P_A\left(S_A\left(M\right)\right) &= M \\ S_A\left(P_A\left(M\right)\right) &= M \end{aligned}$$

In public key cryptography the constraint on S_A is that no one but agent A can compute S_A in any practical amount of time even if P_A is known.

The typical workflow is agent B obtains a representation P_A and use it to encode message M into a ciphertext $C = P_A\left(M\right)$ and then sends it to agent A. Agent A can then apply S_A to recover M, i.e. $S_A\left(C\right) = S_A\left(P_A\left(M\right)\right) = M$. Another workflow is for **digital signatures**: agent A computes her digital signature $\sigma = S_A\left(M'\right)$ for a message she wants to sign and sends $\left(M', \sigma\right)$ to agent B. Agent B then applies $M'' = P_A\left(\sigma\right) = P_A\left(S_A\left(M'\right)\right)$ and compares to M'. If they are indeed equal then the messages is authentic since only agent A could have encoded M' such that $M'' = M'$.

7.2. **RSA.** RSA is based on factorization of large semiprimes. Let $n = pq$, where p, q are prime and e be coprime with $\phi\left(n\right) = \left(p-1\right)\left(q-1\right)$. Then compute the multiplicative inverse d of e modulo $\phi\left(n\right)$, which exists since e is coprime $\phi\left(n\right)$. The public key is then $\left(e, n\right)$ and the private key is $\left(d, n\right)$. These keys specify functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$

$$\begin{aligned} P\left(M\right) &= M^e \mod n \\ S\left(C\right) &= C^d \mod n \end{aligned}$$

Proposition. *With*

$$\begin{aligned} P\left(M\right) &= M^e \mod n \\ S\left(C\right) &= C^d \mod n \end{aligned}$$

it's the case that

$$P\left(S\left(M\right)\right) = \left(\left(M^d\right) \mod n\right)^e \mod n = M^{de} \mod n$$

Proof. Since $ed = 1 + k\phi\left(n\right) = 1 + k\left(p-1\right)\left(q-1\right)$ and if $M \not\equiv_p 0$ then

$$\begin{aligned} M^{ed} &\equiv_p M^{1+k(p-1)(q-1)} \\ &\equiv_p M\left(M^{p-1}\right)^{k(q-1)} \\ &\equiv_p M\left(\left(M \mod p\right)^{p-1}\right)^{k(q-1)} \text{ since the whole thing is } \mod p \text{ anyway} \\ &\equiv_p M\left(1\right)^{k(q-1)} \text{ by Fermat's theorem} \\ &\equiv_p M \end{aligned}$$

Similarly $M^{ed} \equiv_q M$ and therefore by Chinese remainder theorem $M^{ed} \equiv_n M$. □

RSA relies on the difficulty of factoring n. If you are able to factor $n = pq$ of $\left(e, n\right)$ then you can easily compute d in exactly the same way the creator of keys did.

8. Primality Testing

Definition 58. The **prime distribution** function $\pi(n)$ is the number of primes less than or equal to n.

Theorem 59. ***Prime number theorem.***

$$\lim_{n\to\infty}\frac{\pi(n)}{n/\ln(n)} = 1$$

So there are $\approx 48,254,942$ primes less than 10^9. How to figure out whether a number is in fact prime? There is a polynomial time algorithm for doing this but there is a faster probabilistic algorithm called Millar-Rabin.

8.1. Pseudoprimality.

Let $\mathbb{Z}_n^+ = \{1,\dots,n-1\}$. If n is prime then $\mathbb{Z}_n^+ = \mathbb{Z}_n^*$.

Definition 60. n is a **base-a pseudoprime** if n is composite and $a^{n-1} \equiv_n 1$.

Fermat's theorem says that if n is prime then $a^{n-1} \equiv_n 1$ for every $a \in \mathbb{Z}_n^+$. So a base-a pseudoprime is one that tricks you: for some a it's the case that $a^{n-1} \equiv_n 1$ but for some other a' it's the case that $(a')^{n-1} \not\equiv_n 1$. The converse almost holds, i.e. if for $a = 2$ it's the case that $a^{n-1} \equiv_n 1$ then n is probably prime (it could be a base-2 pseudoprime).

Algorithm 2 Primality testing

```
Witness(a, n)
if Modular-Exp(a,n-1,n) ≢_n 1
    return TRUE
else
    return FALSE

Psuedoprime(n)
if Witness(2, n)
    return composite # definitely
else
    return prime # probably (could be psuedoprime)
```

Witness(a, n) returns TRUE if a is a "witness" that n is composite, i.e. $a^{n-1} \not\equiv_n 1$. It's called a witness since it can only confirm that n is composite, not that n is prime. Pseudoprime(n) is correct with fairly high probability. Only 22 in the first 10,000 n are base-2 pseudoprimes. For a 512bit number the chance of Pseudoprime being wrong is 1 in 10^{20} and for a 1024bit number it's 1 in 10^{41}. So if you need large prime numbers (such as for RSA) just pick large numbers until Pseudoprime returns prime.

You can't eliminate all errors by checking against a different base.

Definition 61. A **Carmichael number** n is composite but satisfies $a^{n-1} \equiv_n 1$ for all $a \in \mathbb{Z}_n^*$.

561, 1105, and 1729 are the first 3 Carmichael numbers.

Algorithm 4 Miller-Rabin

```
Miller-Rabin(n, s)
for j = 1 to s
    a = Random(1, n - 1)
    if Witness(a, n)
        return COMPOSITE
return PRIME
```

8.2. **Miller-Rabin.** Miller-Rabin improves on Pseudoprime so that it's not fooled by Carmichael numbers. It tries several bases but also uses the fact that if there exists a nontrivial[4] root of 1 modulo n then n is composite. Hence we update Witness(a, n) to take this into account and we make it more efficient: first pick t and odd u such that $n - 1 = 2^t u$, i.e. factor out as many power of 2 as possible (since n is odd $n - 1$ must be even). Then $a^{n-1} = (a^u)^{2^t}$ and so we can compute $a^{n-1} \mod n$ by computing $a^u \mod n$ first and then squaring the result t times.

Algorithm 3 Witness(a, n)

```
Witness(a, n)
compute t, u as above
x_0 = Modular-Exp(a, u, n)
// do the squaring
for i = 1 to t
    x_i = x_{i-1}^2 mod n
    // test non-trivial square root
    if x_i == 1 and x_{i-1} ≠ ±1
        return TRUE
if x_t ≠ 1
    return TRUE
return FALSE
```

Why does the test $x_i == 1 \wedge x_{i-1} \neq 1 \wedge x_{i-1} \neq n - 1$ return true when x_{i-1} is a nontrivial square root of 1 modulo n? Well duh if $x_i = (x_{i-1})^2 == 1$ but $x_{i-1} \neq 1 \neq -1$ then clearly x_{i-1} is a non-trivial square root[5] of 1 modulo n.

Now Miller-Rabin simply runs Witness(a, n) over and over again

Without proof the error rate of Miller-Rabin(n, s) is at most 2^{-s}.

Exercise 62. If n is composite, then there exists a nontrivial square root of 1 module n.

Proof. Let $n = pq$. The number of roots of $f(x) = x^2 - 1 \equiv_n 0$ is equal to the number product of the number of roots of $f_p(x) = x^2 - 1 \equiv_p 0$ and $f_q(x) = x^2 - 1 \equiv_q 0$. Since each of p, q is prime each of the f_p, f_q has only the trivial roots $1, -1$. So $f(x)$ has $2 \times 2 = 4$ roots and so must have roots other than $-1, 1$. $\square$

[4] i.e. not ± 1.

[5] In the book the test is $x_{i-1} \neq n - 1$ since $-1 \equiv_n n - 1$.

Exercise 63. A strong version of Euler's theorem is that for all $a \in \mathbb{Z}_n^*$

$$a^{\lambda(n)} \equiv_n 1$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ and $\lambda(n) = \operatorname{lcm}\left(\phi\left(p_1^{e_1}\right), \ldots, \phi\left(p_r^{e_r}\right)\right)$.

Proof. Firsly $\lambda(n) \,|\phi(n)$. Why? $\operatorname{lcm}(a,b,c)$ always divides abc so $\operatorname{lcm}(\phi\left(p_1^{e_1}\right), \ldots, \phi\left(p_r^{e_r}\right))$ divides $\phi\left(p_1^{e_1}\right) \cdots \phi\left(p_r^{e_r}\right)$ but

$$\begin{aligned}
\phi(n) &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right) \\
&= p_1^{e_1}\cdots p_r^{e_r}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right) \\
&= \phi\left(p_1^{e_1}\right)\cdots\phi\left(p_r^{e_r}\right)
\end{aligned}$$

and so $\lambda(n) \,|\phi(n)$. Since $a \in \mathbb{Z}_n^*$ it's the case that $\gcd(a,n) = 1$ and so $\gcd\left(a, p_i^{e_i}\right) = 1$ and so

$$a^{\lambda(n)} \equiv_{p_i^{e_i}} 1$$

since $\phi\left(p_i^{e_i}\right) |\lambda(n)$. By the Chinese remainder theorem

$$a^{\lambda(n)} \equiv_n 1$$

□

Exercise 64. If x is nontrivial square root of 1 modulo n then $\gcd(x-1,n)$ and $\gcd(x+1,n)$ are nontrivial divisors of n.

Proof. $n|\left(x-1\right)\left(x+1\right)$. If $\gcd(x-1,n) = n$ then $x \equiv_n 1$, which means x is a trivial square root of 1. So that can't be. Suppose $\gcd(x-1,n) = 1$, then $n|x+1$ and so $x \equiv_n -1$ which means x is a trivial square of 1. So that can't be either. Suppose $\gcd(x+1,n) = n$, then $x \equiv_n -1$, which means x is a trivial root of 1 modulo n. Suppose $\gcd(x+1,n) = 1$, then $n|x-1$ and $x \equiv_n 1$ which shows that x is a trivial root of 1 modulo n. Therefore $\gcd(x+1,n) \neq 1, n$ nor $\gcd(x-1,n) \neq 1, n$. □

8.3. **Cycle finding.** For any function f that maps a finite set S to itself, and any initial value x_0 in S, the sequence of iterated function values

$$x_0, x_1 = f(x_0), x_2 = f(x_1), \ldots, x_i = f(x_{i-1}), \ldots$$

must repeat itself, i.e. there must exist indices $i \neq j$ such that $x_i = x_j$. Note that the values repeat again after the first repetition. That is suppose μ is the first index such that $x_\mu = x_{\mu+\lambda}$ for some λ. Then $x_{\mu+i} = x_{\mu+\lambda+i}$ for $i \geq 0$. That's why it's called a cycle, where λ is the period of length of the cycle. Cycle detection is the problem of finding μ, λ given f, x_0.

The key to solve the problem is realizing that after you hit μ for all k you have $x_i = x_{i+k\lambda}$. In particular when $i = k\lambda$, a multiple of the cycle period, $x_i = x_{k\lambda+k\lambda} = x_{2i}$. So you really only need to look for when values x_i and x_{2i} agree for the first time. At that point $\nu = i$ is equal to the distance between the two pointers and is a multiple of the period of the cycle. To find μ leave one of the pointers where it is so that it has value x_ν, from then on advance it step by step, and reset the other pointer to x_0. Now the distance between them is fixed to be 2ν, a multiple of λ, and so they will agree at the beginning of the cylce, i.e. $x_\mu = x_{\mu+\nu}$. Finding λ after finding μ is easy.

Algorithm 5 Floyd's cycle finding algorithm

```
Floyds(f, x_0)
p_1 = f(x_0)
p_2 = f(p_1)

while p_1 ≠ p_2:
    p_1 = f(p_1)
    p_2 = f(f(p_2))

// p_1 is now at distance ν from the beginning and
// distance ν from p_2. reset p_2 to the beginning.
// even after reset p_1 and p_2 are still distance ν apart
// a multiple of the fundamental period of the cycle.
// advancing one step at a guarantees they'll agree at μ
// since by virtue of because whole periods apart they
// iterate through the same values once they're both on the cycle.
// once p_2 is on the cycle it will agree with p_1.
μ = 0
p_2 = x_0
while p_1 ≠ p_2:
    p_1 = f(p_1)
    p_2 = f(p_2)
    μ = μ + 1

// finding λ is easy now. just advance one
// and wait till they're equal again

p_2 = f(p_1)
λ = 1
while p_1 ≠ p_2:
    p_2 = f(p_2)
    λ = λ + 1
```

8.4. **Pollard's Rho.** Suppose $n = pq$. Randomly select, with replacement, from $S_1 = \{0, 1, 2, \ldots n-1\}$ to form a sequence $x_1, x_2, x_3, \ldots$. Also define a sequence $x_i^{'} = x_i \mod p$, where $x_i^{'} \in S_2 = \{0, 1, 2, \ldots, p-1\}$. Because both S_1, S_2 are finite eventually each of the sequences $x_i, x_i^{'}$ have to repeat eventually, and $x_i^{'}$ should repeat sooner since $|S_2| < |S_1|$. Suppose $x_i^{'} = x_j^{'}$. Then $x_i \equiv_p x_j$ and so $p|x_i - x_j$ and thus $\gcd(|x_i - x_j|, n) \neq 1$ (since at least p divides both). As long as $\gcd(|x_i - x_j|, n) \neq n$ we have found a divisor of n. Note you don't need to compute $x_i \mod p$ (which you can't since you don't know p), but you just have to compute $\gcd(|x_i - x_j|, n)$. I want to be clear about the chain equivalences

$$\begin{array}{rcl} x_i^{'} & = & x_j^{'} \\ & \Longleftrightarrow & \\ x_i & \equiv_p & x_j \\ & \Longleftrightarrow & \\ p & \mid & (x_i - x_j) \\ & \Longleftrightarrow & \\ \gcd(|x_i - x_j|) & \neq & 1 \end{array}$$

So everywhere that you'd want to check whether $x_i \equiv_p x_j$ you just need to check $\gcd(|x_i - x_j|, n)$. Enter Floyd's cycle detection algorithm, which performs the equality check $x_i \equiv_p x_j$. So Pollard's Rho algorithm is just Floyd's cycle detection algorithm but with the $\gcd(|x_i - x_j|, n)$ check replacing $x_i \equiv x_j$, and the function $f(x) = x^2 + 1 \mod n$. Generating x_i using $f(x)$ simulates drawing randomly.

Algorithm 6 Pollard's Rho

```
PollardRho(n)
f(x) = x^2 + 1  mod n
x_0 =  Random(0, n - 1)

p_1 = f(x_0)
p_2 = f(p_1)

while True:
        if 1 < gcd(|p_1 - p_2|, n) < n:
                print |p_1 - p_2|
        p_1 = f(p_1)
        p_2 = f(f(p_2))
```

So what are the chances that picking two numbers from S_1 results in a collision?

Theorem 65. *Birthday Problem. Let $x_0, x_1, \ldots$ be a sequence where x_i is iid random uniform $\{0, 1, \ldots, n-1\}$, and s be the smallest index such that $x_s = x_i$ for some $i < s$. Then $s = O(\sqrt{n})$.*

Proof. The probability that in x_0, x_1, x_2, x_3 no i exists such that $x_i = x_3$ is one minus the probability that it does in x_0, x_1, x_2. The probability that $x_0 = x_3$ is $1/n$, the probability that either $x_0 = x_3$ or $x_1 = x_3$ is $1/n + 1/n = 2/n$, the probability that either $x_0 = x_3$ or $x_1 = x_3$ or $x_2 = x_3$ is $1/n + 1/n + 1/n$. Therefore the probability that in $x_0, \ldots, x_3$ no $i < 3$ exists such that $x_i = x_3$ is

$$1 - \frac{3}{n}$$

Then generalizing for any $j \geq 1$ the probability that for $i < j$ no x_i equals x_j is $\left(1 - \frac{i}{n}\right)$ and so the probability that $s \geq j$ is

$$P(s \geq j) = \prod_{i=0}^{j-1} \left(1 - \frac{i}{n}\right) \leq \prod_{i=0}^{j-1} e^{-i/n} \leq e^{-(j-1)^2/2n}$$

The first inequality comes from the definition of the exponential, the second comes from the integral approximation to the sum. Then

$$\begin{aligned} E[s] &= \sum_{j=0}^{\infty} P[s \geq j] = 1 + \sum_{j=1}^{\infty} P[s \geq j] \\ &\leq 1 + \sum_{j=1}^{\infty} e^{-\frac{(j-1)^2}{2n}} \leq 2 + \sqrt{2n} \int_0^{\infty} e^{-x^2} dx \\ &\leq 2 + \sqrt{2n} \int_0^{\infty} e^{-x} dx = 2 + \sqrt{2n} \end{aligned}$$

and so $E[s] = O(\sqrt{n})$. $\square$

Since $x_i \equiv_p x_j$ is what we're really waiting for is $E[s] = O\left(\sqrt{p}\right)$ and $p = O(\sqrt{n})$ we have that $E[s] = O(\sqrt[4]{n})$.