Chapter 52

Primality testing

By Sariel Har-Peled, April 26, 2022[1]

"The world is what it is; men who are nothing, who allow themselves to become nothing, have no place in it."
— Bend in the river, V.S. Naipaul

Introduction – how to read this write-up

In this note, we present a simple randomized algorithms for primality testing. The challenge is that it requires a non-trivial amount of number theory, which is not the purpose of this course. Nevertheless, this note is more or less self contained, and all necessary background is provided (assuming some basic mathematical familiarity with groups, fields and modulo arithmetic). It is however not really necessary to understand all the number theory material needed, and the reader can take it as given. In particular, I recommend to read the number theory background part without reading all of the proofs (at least on first reading). Naturally, a complete and total understanding of this material one needs to read everything carefully.

The description of the primality testing algorithm in this write-up is not minimal – there are shorter descriptions out there. However, it is modular – assuming the number theory machinery used is correct, the algorithm description is relatively straightforward.

52.1. Number theory background

52.1.1. Modulo arithmetic

52.1.1.1. Prime and coprime

For integer numbers x and y, let $x \mid y$ denotes that x divides y. The *greatest common divisor* (***gcd***) of two numbers x and y, denoted by $\gcd(x, y)$, is the largest integer that divides both x and y. The *least common multiple* (***lcm***) of x and y, denoted by $\operatorname{lcm}(x, y) = xy/\gcd(x, y)$, is the smallest integer α, such that $x \mid \alpha$ and $y \mid \alpha$. An integer number $p > 0$ is ***prime*** if it is divisible only by 1 and itself (we will consider 1 not to be prime).

Some standard definitions:

$$
\begin{aligned}
x, y \text{ are } \textbf{\textit{coprime}} &\iff \gcd(x, y) = 1,\\
\textbf{\textit{quotient}} \text{ of } x/y &\iff x \operatorname{div} y = \lfloor x/y \rfloor,\\
\textbf{\textit{remainder}} \text{ of } x/y &\iff x \bmod y = x - y \lfloor x/y \rfloor.
\end{aligned}
$$

The remainder $x \bmod y$ is sometimes referred to as ***residue***.

52.1.1.2. Computing gcd

```
EuclidGCD(a, b):
    if (b = 0)
        return a
    else
        return EuclidGCD(b, a mod b)
```

Computing the gcd of two numbers is a classical algorithm, see code on the right – proving that it indeed returns the right result follows by an easy induction. It is easy to verify that if the input is made out of $\log n$ bits, then this algorithm takes $O(\operatorname{poly}(\log n))$ time (i.e., it is polynomial in the input size). Indeed, doing basic operations on numbers (i.e., multiplication, division, addition, subtraction, etc) with total of ℓ bits takes $O(\ell^2)$ time (naively – faster algorithms are known).

Exercise 52.1.1. Show that $\gcd(F_n, F_{n-1}) = 1$, where F_i is the ith Fibonacci number. Argue that for two consecutive Fibonacci numbers **EuclidGCD**(F_n, F_{n-1}) takes $O(n)$ time, if every operation takes $O(1)$ time.

Lemma 52.1.2. *For all $\alpha, \beta > 0$ integers, there are integer numbers x and y, such that $\gcd(\alpha, \beta) = \alpha x + \beta y$, which can be computed in polynomial time; that is, $O\Bigl(\operatorname{poly}\Bigl(\log\alpha + \log\beta\Bigr)\Bigr)$.*

Proof: If $\alpha = \beta$ then the claim trivially holds. Otherwise, assume that $\alpha > \beta$ (otherwise, swap them), and observe that $\gcd(\alpha, \beta) = \gcd(\alpha \bmod \beta, \beta)$. In particular, by induction, there are integers x', y', such that $\gcd(\alpha \bmod \beta, \beta) = x'(\alpha \bmod \beta) + y'\beta$. However, $\tau = \alpha \bmod \beta = \alpha - \beta\lfloor \alpha/\beta \rfloor$. As such, we have

$$\gcd(\alpha, \beta) = \gcd(\alpha \bmod \beta, \beta) = x'\Bigl(\alpha - \beta\lfloor \alpha/\beta \rfloor\Bigr) + y'\beta = x'\alpha + (y' - \beta\lfloor \alpha/\beta \rfloor)\beta,$$

as claimed. The running time follows immediately by modifying **EuclidGCD** to compute these numbers. ■

We use $\alpha \equiv \beta \pmod{n}$ or $\alpha \equiv_n \beta$ to denote that α and β are ***congruent modulo n***; that is $\alpha \bmod n = \beta \bmod n$. Or put differently, we have $n \mid (\alpha - \beta)$. The set $\mathbb{Z}_n = \Bigl\{0, \ldots, n-1\Bigr\}$ form a *group* under addition modulo n (see Definition 52.1.9$_{p4}$ for a formal definition of a group). The more interesting creature is $\mathbb{Z}_n^* = \Bigl\{x \Bigm| x \in \{1, \ldots, n\}, x > 0, \text{ and } \gcd(x, n) = 1\Bigr\}$, which is a ***group*** modulo n under multiplication.

Remark 52.1.3. Observe that $\mathbb{Z}_1^* = \{1\}$, while for $n > 1$, $\mathbb{Z}_n^*$ does not contain n.

Lemma 52.1.4. *For any element $\alpha \in \mathbb{Z}_n^*$, there exists a unique inverse element $\beta = \alpha^{-1} \in \mathbb{Z}_n^*$ such that $\alpha * \beta \equiv_n 1$. Furthermore, the inverse can be computed in polynomial time*[②].

Proof: Since $\alpha \in \mathbb{Z}_n^*$, we have that $\gcd(\alpha, n) = 1$. As such, by Lemma 52.1.2, there exists x and y integers, such that $x\alpha + yn = 1$. That is $x\alpha \equiv 1 \pmod{n}$, and clearly $\beta := x \bmod n$ is the desired inverse, and it can be computed in polynomial time by Lemma 52.1.2.

As for uniqueness, assume that there are two inverses β, β' to $\alpha < n$, such that $\beta < \beta' < n$. But then $\beta\alpha \equiv_n \beta'\alpha \equiv_n 1$, which implies that $n \mid (\beta' - \beta)\alpha$, which implies that $n \mid \beta' - \beta$, which is impossible as $0 < \beta' - \beta < n$. ■

It is now straightforward, but somewhat tedious, to verify the following (the interested reader that had not encountered this stuff before can spend some time proving this).

Lemma 52.1.5. *The set $\mathbb{Z}_n$ under the $+$ operation modulo n is a group, as is $\mathbb{Z}_n^*$ under multiplication modulo n. More importantly, for a prime number p, $\mathbb{Z}_p$ forms a field with the $+, *$ operations modulo p (see Definition 52.1.17$_{p6}$).*

[②]Again, as is everywhere in this chapter, the polynomial time is in the number of bits needed to specify the input.

52.1.1.3. The Chinese remainder theorem

Theorem 52.1.6 (Chinese remainder theorem). *Let $n_1, \ldots, n_k$ be coprime numbers, and let $n = n_1 n_2 \cdots n_k$. For any residues $r_1 \in \mathbb{Z}_{n_1}, \ldots, r_k \in \mathbb{Z}_{n_k}$, there is a unique $r \in \mathbb{Z}_n$, which can be computed in polynomial time, such that $r \equiv r_i \pmod{n_i}$, for $i = 1, \ldots, k$.*

Proof: By the coprime property of the n_is it follows that $\gcd(n_i, n/n_i) = 1$. As such, $n/n_i \in \mathbb{Z}^*_{n_i}$, and it has a unique inverse m_i modulo n_i; that is $(n/n_i)m_i \equiv 1 \pmod{n_i}$. So set $r = \sum_i r_i m_i n/n_i$. Observe that for $i \neq j$, we have that $n_j \mid (n/n_i)$, and as such $r_i m_i n/n_i \pmod{n_j} \equiv 0 \pmod{n_j}$. As such, we have

$$r \bmod n_j = \left(\sum_i \left(r_i m_i \frac{n}{n_i} \bmod n_j \right) \right) \bmod n_j = \left(r_j m_j \frac{n}{n_j} \bmod n_j \right) \bmod n_j = r_j * 1 \bmod n_j = r_j.$$

As for uniqueness, if there is another such number r', such that $r < r' < n$, then $r' - r \pmod{n_i} = 0$ implying that $n_i \mid r' - r$, for all i. Since all the n_is are coprime, this implies that $n \mid r' - r$, which is of course impossible. ■

Lemma 52.1.7 (Fast exponentiation). *Given numbers b, c, n, one can compute $b^c \bmod n$ in polynomial time.*

Proof: The key property we need is that

$$xy \bmod n = \Big((x \bmod n)\,(y \bmod n) \Big) \bmod n.$$

Now, if c is even, then we can compute

$$b^c \bmod n = \left(b^{c/2} \right)^2 \bmod n = \left(b^{c/2} \bmod n \right)^2 \bmod n.$$

Similarly, if c is odd, we have

$$b^c \bmod n = (b \bmod n)\left(b^{(c-1)/2} \right)^2 \bmod n = (b \bmod n)\left(b^{(c-1)/2} \bmod n \right)^2 \bmod n.$$

Namely, computing $b^c \bmod n$ can be reduced to recursively computing $b^{\lfloor c/2 \rfloor} \bmod n$, and a constant number of operations (on numbers that are smaller than n). Clearly, the depth of the recursion is $O(\log c)$. ■

52.1.1.4. Euler totient function

The ***Euler totient function*** $\phi(n) = \left|\mathbb{Z}^*_n\right|$ is the number of positive integer numbers that at most n and are coprime with n. If n is prime then $\phi(n) = n - 1$.

Lemma 52.1.8. *Let $n = p_1^{k_1} \cdots p_t^{k_t}$, where the p_is are prime numbers and the k_is are positive integers (this is the* **prime factorization** *of n). Then $\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1)$. and this quantity can be computed in polynomial time if the factorization is given.*

Proof: Observe that $\phi(1) = 1$ (see Remark 52.1.3), and for a prime number p, we have that $\phi(p) = p - 1$. Now, for $k > 1$, and p prime we have that $\phi(p^k) = p^{k-1}(p-1)$, as a number $x \le p^k$ is coprime with p^k, if and only if $x \bmod p \ne 0$, and $(p-1)/p$ fraction of the numbers in this range have this property.

Now, if n and m are relative primes, then $\gcd(x, nm) = 1 \iff \gcd(x, n) = 1$ and $\gcd(x, m) = 1$. In particular, there are $\phi(n)\phi(m)$ pairs $(\alpha, \beta) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$, such that $\gcd(\alpha, n) = 1$ and $\gcd(\beta, m) = 1$. By the Chinese remainder theorem (Theorem 52.1.6), each such pair represents a unique number in the range $1, \ldots, nm$, as desired.

Now, the claim follows by easy induction on the prime factorization of the given number. ■

52.1.2. Structure of the modulo group $\mathbb{Z}_n$

52.1.2.1. Some basic group theory

Definition 52.1.9. A ***group*** is a set, $\mathcal{G}$, together with an operation $\times$ that combines any two elements a and b to form another element, denoted $a \times b$ or ab. To qualify as a group, the set and operation, $(\mathsf{G}, \times)$, must satisfy the following:

(A) (Closure) For all $a, b \in \mathcal{G}$, the result of the operation, $a \times b \in \mathcal{G}$.
(B) (Associativity) For all $a, b, c \in \mathcal{G}$, we have $(a \times b) \times c = a \times (b \times c)$.
(C) (Identity element) There exists an element $\mathsf{i} \in \mathcal{G}$, called the ***identity element***, such that for every element $a \in \mathcal{G}$, the equation $\mathsf{i} \times a = a \times \mathsf{i} = a$ holds.
(D) (Inverse element) For each $a \in \mathcal{G}$, there exists an element $b \in \mathcal{G}$ such that $a \times b = b \times a = \mathsf{i}$.

A group is ***abelian*** (aka, ***commutative group***) if for all $a, b \in \mathcal{G}$, we have that $a \times b = b \times a$.

In the following we restrict our attention to abelian groups since it makes the discussion somewhat simpler. In particular, some of the claims below holds even without the restriction to abelian groups.

The identity element is unique. Indeed, if both $f, g \in \mathcal{G}$ are identity elements, then $f = f \times g = g$. Similarly, for every element $x \in \mathcal{G}$ there exists a unique inverse $y = x^{-1}$. Indeed, if there was another inverse z, then $y = y \times \mathsf{i} = y \times (x \times z) = (y \times x) \times z = \mathsf{i} \times z = z$.

52.1.2.2. Subgroups

For a group $\mathcal{G}$, a subset $\mathcal{H} \subseteq \mathcal{G}$ that is also a group (under the same operation) is a ***subgroup***.

For $x, y \in \mathcal{G}$, let us define $x \sim y$ if $x/y \in \mathcal{H}$. Here $x/y = xy^{-1}$ and y^{-1} is the inverse of y in $\mathcal{G}$. Observe that $(y/x)(x/y) = \left(yx^{-1}\right)\left(xy^{-1}\right) = \mathsf{i}$. That is y/x is the inverse of x/y, and it is in $\mathcal{H}$. But that implies that $x \sim y \implies y \sim x$. Now, if $x \sim y$ and $y \sim z$, then $x/y, y/z \in \mathcal{H}$. But then $x/y \times y/z \in \mathcal{H}$, and furthermore $x/y \times y/z = xy^{-1}yz^{-1} = xz^{-1} = x/z$. that is $x \sim z$. Together, this implies that $\sim$ is an equivalence relationship.

Furthermore, observe that if $x/y = x/z$ then $y^{-1} = x^{-1}(x/y) = x^{-1}(x/z) = z^{-1}$, that is $y = z$. In particular, the equivalence class of $x \in \mathcal{G}$, is $[x] = \left\{ z \in \mathcal{G} \,\middle|\, x \sim z \right\}$. Observe that if $x \in \mathcal{H}$ then $\mathsf{i}/x = \mathsf{i}x^{-1} = x^{-1} \in \mathcal{H}$, and thus $\mathsf{i} \sim x$. That is $\mathcal{H} = [x]$. The following is now easy.

Lemma 52.1.10. *Let $\mathcal{G}$ be an abelian group, and let $\mathcal{H} \subseteq \mathcal{G}$ be a subgroup. Consider the set $\mathcal{G}/\mathcal{H} = \left\{ [x] \,\middle|\, x \in \mathcal{G} \right\}$. We claim that $\left|[x]\right| = \left|[y]\right|$ for any $x, y \in \mathcal{G}$. Furthermore $\mathcal{G}/\mathcal{H}$ is a group (that is, the* **quotient group***), with $[x] \times [y] = [x \times y]$.*

Proof: Pick an element $\alpha \in [x]$, and $\beta \in [y]$, and consider the mapping $f(x) = x\alpha^{-1}\beta$. We claim that f is one to one and onto from $[x]$ to $[y]$. For any $\gamma \in [x]$, we have that $\gamma\alpha^{-1} = \gamma/\alpha \in \mathcal{H}$ As such, $f(\gamma) = \gamma\alpha^{-1}\beta \in [\beta] = [y]$. Now, for any $\gamma, \gamma' \in [x]$ such that $\gamma \ne \gamma'$, we have that if

$f(\gamma) = \gamma\alpha^{-1}\beta = \gamma'\alpha^{-1}\beta = f(\gamma')$, then by multiplying by $\beta^{-1}\alpha$, we have that $\gamma = \gamma'$. That is, f is one to one, implying that $\left|[x]\right| = \left|[y]\right|$.

The second claim follows by careful but tediously checking that the conditions in the definition of a group holds. ∎

Lemma 52.1.11. *For a finite abelian group $\mathcal{G}$ and a subgroup $\mathcal{H} \subseteq \mathcal{G}$, we have that $|\mathcal{H}|$ divides $|\mathcal{G}|$.*

Proof: By Lemma 52.1.10, we have that $|\mathcal{G}| = |\mathcal{H}| \cdot |\mathcal{G}/\mathcal{H}|$, as $\mathcal{H} = [\mathsf{i}]$. ∎

52.1.2.3. Cyclic groups

Lemma 52.1.12. *For a finite group $\mathcal{G}$, and any element $g \in \mathcal{G}$, the set $\langle g \rangle = \left\{ g^i \,\middle|\, i \geq 0 \right\}$ is a group.*

Proof: Since $\mathcal{G}$ is finite, there are integers $i > j \geq 1$, such that $i \neq j$ and $g^i = g^j$, but then $g^j \times g^{i-j} = g^i = g^j$. That is $g^{i-j} = \mathsf{i}$ and, by definition, we have $g^{i-j} \in \langle g \rangle$. It is now straightforward to verify that the other properties of a group hold for $\langle g \rangle$. ∎

In particular, for an element $g \in \mathcal{G}$, we define its ***order*** as $\mathrm{ord}(g) = \left|\langle g \rangle\right|$, which clearly is the minimum positive integer m, such that $g^m = \mathsf{i}$. Indeed, for $j > m$, observe that $g^j = g^{j \bmod m} \in X = \left\{\mathsf{i}, g, g^2, \ldots, g^{m-1}\right\}$, which implies that $\langle g \rangle = X$.

A group $\mathcal{G}$ is ***cyclic***, if there is an element $g \in \mathcal{G}$, such that $\langle g \rangle = \mathcal{G}$. In such a case g is a ***generator*** of $\mathcal{G}$.

Lemma 52.1.13. *For any finite abelian group $\mathcal{G}$, and any $g \in \mathcal{G}$, we have that $\mathrm{ord}(g)$ divides $|\mathcal{G}|$, and $g^{|\mathcal{G}|} = \mathsf{i}$.*

Proof: By Lemma 52.1.12, the set $\langle g \rangle$ is a subgroup of $\mathcal{G}$. By Lemma 52.1.11, we have that $\mathrm{ord}(g) = \left|\langle g \rangle\right| \mid |\mathcal{G}|$. As such, $g^{|\mathcal{G}|} = \left(g^{\mathrm{ord}(g)}\right)^{|\mathcal{G}|/\mathrm{ord}(g)} = \left(\mathsf{i}\right)^{|\mathcal{G}|/\mathrm{ord}(g)} = \mathsf{i}$. ∎

52.1.2.4. Modulo group

Lemma 52.1.14. *For any integer n, consider the additive group $\mathbb{Z}_n$. Then, for any $x \in \mathbb{Z}_n$, we have that $x \cdot \mathrm{ord}(x) = \mathrm{lcm}(x, n)$. In particular, $\mathrm{ord}(x) = \dfrac{\mathrm{lcm}(n, x)}{x} = \dfrac{n}{\gcd(n, x)}$. If n is prime, and $x \neq 0$ then $\mathrm{ord}(x) = |\mathbb{Z}_n| = n$, and $\mathbb{Z}_n$ is a cyclic group.*

Proof: We are working modulo n here under additions, and the identity element is 0. As such, $x \cdot \mathrm{ord}(x) \equiv_n 0$, which implies that $n \mid x\,\mathrm{ord}(x)$. By definition, $\mathrm{ord}(x)$ is the minimal number that has this property, implying that $\mathrm{ord}(x) = \dfrac{\mathrm{lcm}(n, x)}{x}$. Now, $\mathrm{lcm}(n, x) = nx/\gcd(n, x)$. The second claim is now easy. ∎

Theorem 52.1.15. ***(Euler's theorem)*** *For all n and $x \in \mathbb{Z}_n^*$, we have $x^{\phi(n)} \equiv 1 \pmod{n}$.*

(Fermat's theorem) *If p is a prime then $\forall x \in \mathbb{Z}_p^* \quad x^{p-1} \equiv 1 \pmod{p}$.*

Proof: The group $\mathbb{Z}_n^*$ is abelian and has $\phi(n)$ elements, with 1 being the identity element (duh!). As such, by Lemma 52.1.13, we have that $x^{\phi(n)} = x^{|\mathbb{Z}_n^*|} \equiv 1 \pmod{n}$, as claimed.

The second claim follows by setting $n = p$, and recalling that $\phi(p) = p - 1$, if p is a prime. ∎

One might be tempted to think that Lemma 52.1.14 implies that if p is a prime then $\mathbb{Z}_p^*$ is a cyclic group, but this does not follow, as the cardinality of $\mathbb{Z}_p^*$ is $\phi(p) = p - 1$, which is not a prime number (for $p > 2$). To prove that $\mathbb{Z}_p^*$ is cyclic, let us go back shortly to the totient function.

Lemma 52.1.16. *For any $n > 0$, we have $\sum_{d|n} \phi(d) = n$.*

Proof: For any $g > 0$, let $V_g = \left\{ x \;\middle|\; x \in \{1, \ldots, n\} \text{ and } \gcd(x, n) = g \right\}$. Now, $x \in V_g \iff \gcd(x, n) = g \iff \gcd(x/g, n/g) = 1 \iff x/g \in \mathbb{Z}_{n/g}^*$. Since $V_1, V_2, \ldots, V_n$ form a partition of $\{1, \ldots, n\}$, it follows that $n = \sum_g |V_g| = \sum_{g|n} \left|\mathbb{Z}_{n/g}^*\right| = \sum_{g|n} \phi(n/g) = \sum_{d|n} \phi(d)$. ■

52.1.2.5. Fields

Definition 52.1.17. A ***field*** is an algebraic structure $\langle \mathbb{F}, +, *, 0, 1 \rangle$ consisting of two abelian groups:

(A) $\mathbb{F}$ under $+$, with 0 being the identity element.

(B) $\mathbb{F} \setminus \{0\}$ under $*$, with 1 as the identity element (here $0 \neq 1$).

Also, the following property (***distributivity of multiplication over addition***) holds:

$$\forall a, b, c \in \mathbb{F} \qquad a * (b + c) = (a * b) + (a * c).$$

We need the following: A polynomial p of degree k over a field $\mathbb{F}$ has at most k roots. indeed, if p has the root α then it can be written as $p(x) = (x - \alpha)q(x)$, where $q(x)$ is a polynomial of one degree lower. To see this, we divide $p(x)$ by the polynomial $(x - \alpha)$, and observe that $p(x) = (x - \alpha)q(x) + \beta$, but clearly $\beta = 0$ since $p(\alpha) = 0$. As such, if p had t roots $\alpha_1, \ldots, \alpha_t$, then $p(x) = q(x) \prod_{i=1}^{t} (x - \alpha_i)$, which implies that p would have degree at least t.

52.1.2.6. $\mathbb{Z}_p^*$ is cyclic for prime numbers

For a prime number p, the group $\mathbb{Z}_p^*$ has size $\phi(p) = p - 1$, which is not a prime number for $p > 2$. As such, Lemma 52.1.13 does not imply that there must be an element in $\mathbb{Z}_p^*$ that has order $p - 1$ (and thus $\mathbb{Z}_p^*$ is cyclic). Instead, our argument is going to be more involved and less direct.

Lemma 52.1.18. *For $k < n$, let $R_k = \left\{ x \in \mathbb{Z}_p^* \;\middle|\; \mathrm{ord}(x) = k \right\}$ be the set of all numbers in $\mathbb{Z}_p^*$ that are of order k. We have that $|R_k| \leq \phi(k)$.*

Proof: Clearly, all the elements of R_k are roots of the polynomial $x^k - 1 = 0 \pmod n$. By the above, this polynomial has at most k roots. Now, if R_k is not empty, then it contains an element $x \in R_k$ of order k, which implies that for all $i < j \leq k$, we have that $x^i \not\equiv x^j \pmod n$, as the order of x is the size of $\langle x \rangle$, and the minimum k such that $x^k \equiv 1 \pmod n$. In particular, we have that $R_k \subseteq \langle x \rangle$, as for $y = x^j$, we have that $y^k \equiv_n x^{jk} \equiv_n 1^j \equiv_n 1$.

Observe that for $y = x^i$, if $g = \gcd(k, i) > 1$, then $y^{k/g} \equiv_n x^{i(k/g)} \equiv_n x^{\mathrm{lcm}(i,k)} \equiv_n 1$; that is, $\mathrm{ord}(y) \leq k/g < k$, and $y \notin R_k$. As such, R_k contains only elements of x^i such that $\gcd(i, k) = 1$. That is $R_k \subseteq \mathbb{Z}_k^*$. The claim now readily follows as $\left|\mathbb{Z}_k^*\right| = \phi(k)$. ■

Lemma 52.1.19. *For any prime p, the group $\mathbb{Z}_p^*$ is cyclic.*

Proof: For $p = 2$ the claim trivially holds, so assume $p > 2$. If the set R_{p-1}, from Lemma 52.1.18, is not empty, then there is $g \in R_{p-1}$, it has order $p - 1$, and it is a generator of $\mathbb{Z}_p^*$, as $\left|\mathbb{Z}_p^*\right| = p - 1$, implying that $\mathbb{Z}_p^* = \langle g \rangle$ and this group is cyclic.

Now, by Lemma 52.1.13, we have that for any $y \in \mathbb{Z}_p^*$, we have that $\mathrm{ord}(y) \mid p - 1 = \left|\mathbb{Z}_p^*\right|$. This implies that R_k is empty if k does not divides $p - 1$. On the other hand, $R_1, \ldots, R_{p-1}$ form a partition of $\mathbb{Z}_p^*$. As such, we have that

$$p - 1 = \left|\mathbb{Z}_p^*\right| = \sum_{k \mid p-1} |R_k| \leq \sum_{k \mid p-1} \phi(k) = p - 1,$$

by Lemma 52.1.18 and Lemma 52.1.16$_{\text{p6}}$, implying that the inequality in the above display is equality, and for all $k \mid p - 1$, we have that $|R_k| = \phi(k)$. In particular, $\left|R_{p-1}\right| = \phi(p - 1) > 0$, and by the above the claim follows. ■

52.1.2.7. $\mathbb{Z}_n^*$ is cyclic for powers of a prime

Lemma 52.1.20. *Consider any odd prime p, and any integer $c \geq 1$, then the group $\mathbb{Z}_n^*$ is cyclic, where $n = p^c$.*

Proof: Let g be a generator of $\mathbb{Z}_p^*$. Observe that $g^{p-1} \equiv 1 \mod p$. The number $g < p$, and as such p does not divide g, and also p does not divide g^{p-2}, and also p does not divide $p - 1$. As such, p^2 does not divide $\Delta = (p - 1)g^{p-2}p$; that is, $\Delta \not\equiv 0 \pmod{p^2}$. As such, we have that

$$\begin{aligned} & (g + p)^{p-1} \equiv g^{p-1} + \binom{p-1}{1} g^{p-2} p \equiv g^{p-1} + \Delta \not\equiv g^{p-1} \pmod{p^2} \\ \implies \quad & (g + p)^{p-1} \not\equiv 1 \pmod{p^2} \qquad \text{or} \qquad g^{p-1} \not\equiv 1 \pmod{p^2}. \end{aligned}$$

Renaming $g + p$ to be g, if necessary, we have that $g^{p-1} \not\equiv 1 \pmod{p^2}$, but by Theorem 52.1.15$_{\text{p5}}$, $g^{p-1} \equiv 1 \pmod{p}$. As such, $g^{p-1} = 1 + \beta p$, where p does not divide β. Now, we have

$$g^{p(p-1)} = (1 + \beta p)^p = 1 + \binom{p}{1} \beta p + \beta p^3 \text{<whatever>} = 1 + \gamma_1 p^2,$$

where γ_1 is an integer (the p^3 is not a typo – the binomial coefficient contributes at least one factor of p – here we are using that $p > 2$). In particular, as p does not divides β, it follows that p does not divides γ_1 either. Let us apply this argumentation again to

$$g^{p^2(p-1)} = \left(1 + \gamma_1 p^2\right)^p = 1 + \gamma_1 p^3 + p^4 \text{<whatever>} = 1 + \gamma_2 p^3,$$

where again p does not divides γ_2. Repeating this argument, for $i = 1, \ldots, c - 2$, we have

$$\alpha_i = g^{p^i(p-1)} = \left(g^{p^{i-1}(p-1)}\right)^p = \left(1 + \gamma_{i-1} p^i\right)^p = 1 + \gamma_{i-1} p^{i+1} + p^{i+2} \text{<whatever>} = 1 + \gamma_i p^{i+1},$$

where p does not divides γ_i. In particular, this implies that $\alpha_{c-2} = 1 + \gamma_{c-2} p^{c-1}$ and p does not divides γ_{c-2}. This in turn implies that $\alpha_{c-2} \not\equiv 1 \pmod{p^c}$.

Now, the order of g in $\mathbb{Z}_n$, denoted by k, must divide $\left|\mathbb{Z}_n^*\right|$ by Lemma 52.1.13$_{\text{p5}}$. Now $\left|\mathbb{Z}_n^*\right| = \phi(n) = p^{c-1}(p - 1)$, see Lemma 52.1.8$_{\text{p3}}$. So, $k \mid p^{c-1}(p - 1)$. Also, $\alpha_{c-2} \not\equiv 1 \pmod{p^c}$. implies that k does not divides $p^{c-2}(p - 1)$. It follows that $p^{c-1} \mid k$. So, let us write $k = p^{c-1}k'$, where $k' \leq (p - 1)$. This, by definition, implies that $g^k \equiv 1 \pmod{p^c}$. Now, $g^p \equiv g \pmod{p}$, because g is a generator of $\mathbb{Z}_p^*$. As such, we have that

$$g^k \equiv_p g^{p^\delta k'} \equiv_p (g^p)^{p^{\delta-1}k'} \equiv_p (g)^{p^{\delta-1}k'} \equiv_p \ldots \equiv_p (g)^{k'} \equiv_p \left(g^k \bmod p^c\right) \bmod p \equiv_p 1.$$

Namely, $g^{k'} \equiv 1 \pmod{p}$, which implies, as g as a generator of $\mathbb{Z}_p^*$, that either $k' = 1$ or $k' = p - 1$. The case $k' = 1$ is impossible, as this implies that $g = 1$, and it can not be the generator of $\mathbb{Z}_p^*$. We conclude that $k = p^{c-1}(p-1)$; that is, $\mathbb{Z}_n^*$ is cyclic. ■

52.1.3. Quadratic residues

52.1.3.1. Quadratic residue

Definition 52.1.21. An integer α is a ***quadratic residue*** modulo a positive integer n, if $\gcd(\alpha, n) = 1$ and for some integer β, we have $\alpha \equiv \beta^2 \pmod{n}$.

Theorem 52.1.22 (Euler's criterion). *Let p be an odd prime, and $\alpha \in \mathbb{Z}_p^*$. We have that*

(A) $\alpha^{(p-1)/2} \equiv_p \pm 1$.
(B) If α is a quadratic residue, then $\alpha^{(p-1)/2} \equiv_p 1$.
(C) If α is not a quadratic residue, then $\alpha^{(p-1)/2} \equiv_p -1$.

Proof: (A) Let $\gamma = \alpha^{(p-1)/2}$, and observe that $\gamma^2 \equiv_p \alpha^{p-1} \equiv 1$, by Fermat's theorem (Theorem 52.1.15$_{\text{p5}}$), which implies that γ is either $+1$ or -1, as the polynomial $x^2 - 1$ has at most two roots over a field.

(B) Let $\alpha \equiv_p \beta^2$, and again by Fermat's theorem, we have $\alpha^{(p-1)/2} \equiv_p \beta^{p-1} \equiv_p 1$.

(C) Let X be the set of elements in $\mathbb{Z}_p^*$ that are not quadratic residues, and consider $\alpha \in X$. Since $\mathbb{Z}_p^*$ is a group, for any $x \in \mathbb{Z}_p^*$ there is a unique $y \in \mathbb{Z}_p^*$ such that $xy \equiv_p \alpha$. As such, we partition $\mathbb{Z}_p^*$ into pairs $C = \left\{\{x, y\} \;\middle|\; x, y \in \mathbb{Z}_p^* \text{ and } xy \equiv_p \alpha\right\}$. We have that

$$\tau \equiv_p \prod_{\beta \in \mathbb{Z}_p^*} \beta \equiv_p \prod_{\{x,y\} \in C} xy \equiv_p \prod_{\{x,y\} \in C} \alpha \equiv_p \alpha^{(p-1)/2}.$$

Let consider a similar set of pair, but this time for 1: $D = \left\{\{x, y\} \;\middle|\; x, y \in \mathbb{Z}_p^*, x \neq y \text{ and } xy \equiv_p 1\right\}$. Clearly, D does not contain -1 and 1, but all other elements in $\mathbb{Z}_p^*$ are in D. As such,

$$\tau \equiv_p \prod_{\beta \in \mathbb{Z}_p^*} \beta \equiv_p (-1)1 \prod_{\{x,y\} \in D} xy \equiv_p \prod_{\{x,y\} \in D} 1 \equiv_p -1.$$ ■

52.1.3.2. Legendre symbol

For an odd prime p, and an integer a with $\gcd(a, n) = 1$, the ***Legendre symbol*** $(a \mid p)$ is one if a is a quadratic residue modulo p, and -1 otherwise (if $p \mid a$, we define $(a \mid p) = 0$). Euler's criterion (Theorem 52.1.22) implies the following equivalent definition.

Definition 52.1.23. The ***Legendre symbol***, for a prime number p, and $a \in \mathbb{Z}_p^*$, is

$$(a \mid p) = a^{(p-1)/2} \pmod{p}.$$

The following is easy to verify.

Lemma 52.1.24. *Let p be an odd prime, and let a, b be integer numbers. We have:*
(i) $(-1 \mid p) = (-1)^{(p-1)/2}$.
(ii) $(a \mid p)\,(b \mid p) = (ab \mid p)$.
(iii) If $a \equiv_p b$ *then* $(a \mid p) = (b \mid p)$.

Lemma 52.1.25 (Gauss' lemma). *Let p be an odd prime and let a be an integer that is not divisible by p. Let $X = \left\{\alpha_j = ja \pmod p \,\middle|\, j = 1, \ldots, (p-1)/2\right\}$, and $L = \left\{x \in X \,\middle|\, x > p/2\right\} \subseteq X$. Then $(a \mid p) = (-1)^n$, where $n = |L|$.*

Proof: Observe that for any distinct i, j, such that $1 \leq i \leq j \leq (p-1)/2$, we have that $ja \equiv ia \pmod p$ implies that $(j-i)a \equiv 0 \pmod p$, which is impossible as $j - i < p$ and $\gcd(a, p) = 1$. As such, all the elements of X are distinct, and $|X| = (p-1)/2$. We have a somewhat stronger property: If $ja \equiv p - ia \pmod p$ implies $(j+i)a \equiv 0 \pmod p$, which is impossible. That is, $S = X \setminus L$, and $\overline{L} = \left\{p - \ell \,\middle|\, \ell \in L\right\}$ are disjoint, and $S \cup \overline{L} = \left\{1, \ldots, (p-1)/2\right\}$. As such,

$$\left(\frac{p-1}{2}\right)! \;\equiv \prod_{x \in S} x \cdot \prod_{y \in L} (p - y) \;\equiv\; (-1)^n \prod_{x \in S} x \cdot \prod_{y \in L} y \;\equiv\; (-1)^n \prod_{j=1}^{(p-1)/2} ja \equiv\; (-1)^n a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod p.$$

Dividing both sides by $(-1)^n((p-1)/2)!$, we have that $(a \mid p) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod p$, as claimed. ∎

Lemma 52.1.26. *If p is an odd prime, and $a > 2$ and $\gcd(a, p) = 1$ then $(a \mid p) = (-1)^\Delta$, where $\Delta = \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor$. Furthermore, we have $(2 \mid p) = (-1)^{(p^2-1)/8}$.*

Proof: Using the notation of Lemma 52.1.25, we have

$$\begin{aligned}\sum_{j=1}^{(p-1)/2} ja &= \sum_{j=1}^{(p-1)/2} \Big(\lfloor ja/p \rfloor\, p + (ja \bmod p) \Big) = \Delta p + \sum_{x \in S} x + \sum_{y \in L} y = (\Delta + n)p + \sum_{x \in S} x - \sum_{y \in \overline{L}} y \\ &= (\Delta + n)p + \sum_{j=1}^{(p-1)/2} j - 2 \sum_{y \in \overline{L}} y.\end{aligned}$$

Rearranging, and observing that $\sum_{j=1}^{(p-1)/2} j = \frac{p-1}{2} \cdot \frac{1}{2}\left(\frac{p-1}{2} + 1\right) = \frac{p^2-1}{8}$. We have that

$$(a-1)\frac{p^2-1}{8} = (\Delta + n)p - 2\sum_{y \in \overline{L}} y. \qquad \Longrightarrow \qquad (a-1)\frac{p^2-1}{8} \equiv (\Delta + n)p \pmod 2. \tag{52.1}$$

Observe that $p \equiv 1 \pmod 2$, and for any x we have that $x \equiv -x \pmod 2$. As such, and if a is odd, then the above implies that $n \equiv \Delta \pmod 2$. Now the claim readily follows from Lemma 52.1.25.

As for $(2 \mid p)$, setting $a = 2$, observe that $\lfloor ja/p \rfloor = 0$, for $j = 0, \ldots (p-1)/2$, and as such $\Delta = 0$. Now, Eq. (52.1) implies that $\frac{p^2-1}{8} \equiv n \pmod 2$, and the claim follows from Lemma 52.1.25. ∎

Theorem 52.1.27 (***Law of quadratic reciprocity***)**.** *If p and q are distinct odd primes, then*

$$(p \mid q) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (q \mid p).$$

Proof: Let $S = \left\{(x,y) \,\middle|\, 1 \le x \le (p-1)/2 \text{ and } 1 \le y \le (q-1)/2\right\}$. As $\mathrm{lcm}(p,q) = pq$, it follows that there are no $(x,y) \in S$, such that $qx = py$, as all such numbers are strict smaller than pq. Now, let

$$S_1 = \left\{(x,y) \in S \,\middle|\, qx > py\right\} \qquad \text{and} \qquad S_2 = \left\{(x,y) \in S \,\middle|\, qx < py\right\}.$$

Now, $(x,y) \in S_1 \iff 1 \le x \le (p-1)$, and $1 \le y \le \lfloor qx/p \rfloor$. As such, we have $|S_1| = \sum_{x=1}^{(p-1)/2} \lfloor qx/p \rfloor$, and similarly $|S_2| = \sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor$. We have

$$\tau = \frac{p-1}{2} \cdot \frac{q-1}{2} = |S| = |S_1| + |S_2| = \underbrace{\sum_{x=1}^{(p-1)/2} \lfloor qx/p \rfloor}_{\tau_1} + \underbrace{\sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor}_{\tau_2}.$$

The claim now readily follows by Lemma 52.1.26, as $(-1)^\tau = (-1)^{\tau_1}(-1)^{\tau_2} = (p \mid q)\,(q \mid p)$. ∎

52.1.3.3. Jacobi symbol

Definition 52.1.28. For any integer a, and an odd number n with prime factorization $n = p_1^{k_1} \cdots p_t^{k_t}$, its ***Jacobi symbol*** is

$$[\![a \mid n]\!] = \prod_{i=1}^{t} (a \mid p_i)^{k_i}.$$

Claim 52.1.29. *For odd integers $n_1, \ldots, n_k$, we have that $\sum_{i=1}^{k}(n_i - 1)/2 \equiv \left(\prod_{i=1}^{k} n_i - 1\right)/2 \pmod 2$.*

Proof: We prove for two odd integers x and y, and apply this repeatedly to get the claim. Indeed, we have $\frac{x-1}{2} + \frac{y-1}{2} \equiv \frac{xy-1}{2} \pmod 2 \iff 0 \equiv \frac{xy - x + 1 - y + 1 - 1}{2} \pmod 2 \iff 0 \equiv \frac{xy - x - y + 1}{2} \pmod 2 \iff 0 \equiv \frac{(x-1)(y-1)}{2} \pmod 2$, which is obviously true. ∎

Lemma 52.1.30 (***Law of quadratic reciprocity***)**.** *For n and m positive odd integers, we have that $[\![n \mid m]\!] = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} [\![m \mid n]\!]$.*

Proof: Let $n = \prod_{i=1}^{\nu} p_i$ and Let $m = \prod_{j=1}^{\mu} q_j$ be the prime factorization of the two numbers (allowing repeated factors). If they share a common factor p, then both $[\![n \mid m]\!]$ and $[\![m \mid n]\!]$ contain a zero term when expanded, as $(n \mid p) = (m \mid p) = 0$. Otherwise, we have

$$\begin{aligned}
[\![n \mid m]\!] &= \prod_{i=1}^{\nu}\prod_{j=1}^{\mu} [\![p_i \mid q_j]\!] = \prod_{i=1}^{\nu}\prod_{j=1}^{\mu} (p_i \mid q_j) = \prod_{i=1}^{\nu}\prod_{j=1}^{\mu} (-1)^{(q_j-1)/2 \cdot (p_i-1)/2} (q_j \mid p_i) \\
&= \underbrace{\prod_{i=1}^{\nu}\prod_{j=1}^{\mu} (-1)^{(q_j-1)/2 \cdot (p_i-1)/2}}_{s} \cdot \left(\prod_{i=1}^{\nu}\prod_{j=1}^{\mu} (q_j \mid p_i)\right) = s\,[\![m \mid n]\!].
\end{aligned}$$

by Theorem 52.1.27. As for the value of s, observe that

$$s = \prod_{i=1}^{\nu} \left(\prod_{j=1}^{\mu} (-1)^{(q_j-1)/2} \right)^{(p_i-1)/2} = \prod_{i=1}^{\nu} \left((-1)^{(m-1)/2} \right)^{(p_i-1)/2} = \left(\prod_{i=1}^{\nu} (-1)^{(p_i-1)/2} \right)^{(m-1)/2} = (-1)^{(n-1)/2 \cdot (m-1)/2},$$

by repeated usage of Claim 52.1.29. ∎

Lemma 52.1.31. *For odd integers n and m, we have that* $\dfrac{n^2-1}{8} + \dfrac{m^2-1}{8} \equiv \dfrac{n^2m^2-1}{8} \pmod 2$.

Proof: For an odd integer n, we have that either (i) $2 \mid n-1$ and $4 \mid n+1$, or (ii) $4 \mid n-1$ and $2 \mid n+1$. As such, $8 \mid n^2 - 1 = (n-1)(n+1)$. In particular, $64 \mid \left(n^2-1\right)\left(m^2-1\right)$. We thus have that

$$\begin{aligned} \frac{\left(n^2-1\right)\left(m^2-1\right)}{8} \equiv 0 \pmod 2 &\iff \frac{n^2m^2 - n^2 - m^2 + 1}{8} \equiv 0 \pmod 2 \\ &\iff \frac{n^2m^2-1}{8} \equiv \frac{n^2 - m^2 - 2}{8} \pmod 2 \\ &\iff \frac{n^2-1}{8} + \frac{m^2-1}{8} \equiv \frac{n^2m^2-1}{8} \pmod 2. \end{aligned}$$

∎

Lemma 52.1.32. *Let m, n be odd integers, and a, b be any integers. We have the following:*

(A) $[\![ab \mid n]\!] = [\![a \mid n]\!]\,[\![b \mid n]\!]$.
(B) $[\![a \mid nm]\!] = [\![a \mid n]\!]\,[\![a \mid m]\!]$.
(C) If $a \equiv b \pmod n$ *then* $[\![a \mid n]\!] = [\![b \mid n]\!]$.
(D) If $\gcd(a,n) > 1$ *then* $[\![a \mid n]\!] = 0$.
(E) $[\![1 \mid n]\!] = 1$.
(F) $[\![2 \mid n]\!] = (-1)^{(n^2-1)/8}$.
(G) $[\![n \mid m]\!] = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\,[\![m \mid n]\!]$.

Proof: (A) Follows immediately, as $(ab \mid p_i) = (a \mid p_i)\,(b \mid p_i)$, see Lemma 52.1.24$_{\text{p9}}$.

(B) Immediate from definition.

(C) Follows readily from Lemma 52.1.24$_{\text{p9}}$ (iii).

(D) Indeed, if $p \mid \gcd(a,n)$ and $p > 1$, then $(a \mid p)^k = (0 \mid p)^k = 0$ appears as a term in $[\![a \mid n]\!]$.

(E) Obvious by definition.

(F) By Lemma 52.1.26$_{\text{p9}}$, for a prime p, we have $(2 \mid p) = (-1)^{(p^2-1)/8}$. As such, writing $n = \prod_{i=1}^{t} p_i$ as a product of primes (allowing repeated primes), we have

$$[\![2 \mid n]\!] = \prod_{i=1}^{t} (2 \mid p_i) = \prod_{i=1}^{t} (-1)^{(p_i^2-1)/8} = (-1)^{\Delta},$$

where $\Delta = \sum_{i=1}^{t} (p_i^2 - 1)/8$. As such, we need to compute the $\Delta \pmod 2$, which by Lemma 52.1.31, is

$$\Delta \equiv \sum_{i=1}^{t} \frac{p_i^2-1}{8} \equiv \frac{\prod_{i=1}^{t} p_i^2 - 1}{8} \equiv \frac{n^2-1}{8} \pmod 2,$$

and as such $[\![2 \mid n]\!] = (-1)^{\Delta} = (-1)^{(n^2-1)/8}$.

(G) This is Lemma 52.1.30. ∎

52.1.3.4. Jacobi(a, n): Computing the Jacobi symbol

Given a and n (n is an odd number), we are interested in computing (in polynomial time) the Jacobi symbol $[\![a \mid n]\!]$. The algorithm **Jacobi**(a, n) works as follows:

(A) If $a = 0$ then **return** 0 `// Since` $[\![0 \mid n]\!] = 0$.
(B) If $a > n$ then **return** **Jacobi**$(a \pmod n, n)$ `// Lemma 52.1.32 (C)`
(C) If $\gcd(a, n) > 1$ then **return** 0 `// Lemma 52.1.32 (D)`
(D) If $a = 2$ then

  (I) Compute $\Delta = n^2 - 1 \pmod{16}$,
  (II) Return $(-1)^{\Delta/8 \pmod 2}$ `// As` $(n^2-1)/8 \equiv \Delta/8 \pmod 2$`, and by Lemma 52.1.32 (F)`

(E) If $2 \mid a$ then **return** **Jacobi**$(2, n)$ * **Jacobi**$(a/2, n)$ `// Lemma 52.1.32 (A)`

  `// Must be that` a `and` b `are both odd,` $a < n$`, and they are coprime`
(F) $a' := a \pmod 4$, $n' := n \pmod 4$, $\beta = (a'-1)(n'-1)/4$.

  return $(-1)^{\beta}$ **Jacobi**(n, a) `// By Lemma 52.1.32 (G)`

Ignoring the recursive calls, all the operations takes polynomial time. Clearly, computing **Jacobi**$(2, n)$ takes polynomial time. Otherwise, observe that **Jacobi** reduces its input size by say, one bit, at least every two recursive calls, and except the $a = 2$ case, it always perform only a single call. Thus, it follows that its running time is polynomial. We thus get the following.

Lemma 52.1.33. *Given integers a and n, where n is odd, then $[\![a \mid n]\!]$ can be computed in polynomial time.*

52.1.3.5. Subgroups induced by the Jacobi symbol

For an n, consider the set

$$J_n = \left\{ a \in \mathbb{Z}_n^* \;\middle|\; [\![a \mid n]\!] \equiv a^{(n-1)/2} \bmod n \right\}. \tag{52.2}$$

Claim 52.1.34. *The set J_n is a subgroup of $\mathbb{Z}_n^*$.*

Proof: For $a, b \in J_n$, we have that $[\![ab \mid n]\!] \equiv [\![a \mid n]\!]\,[\![b \mid n]\!] \equiv a^{(n-1)/2} b^{(n-1)/2} \equiv (ab)^{(n-1)/2} \bmod n$, implying that $ab \in J_n$. Now, $[\![1 \mid n]\!] = 1$, so $1 \in J_n$. Now, for $a \in J_n$, let a^{-1} the inverse of a (which is a number in $\mathbb{Z}_n^*$). Observe that $a(a^{-1}) = kn + 1$, for some k, and as such, we have

$$1 = [\![1 \mid n]\!] = [\![kn+1 \mid n]\!] = [\![aa^{-1} \mid n]\!] = [\![kn+1 \mid n]\!] = [\![a \mid n]\!]\,[\![a^{-1} \mid n]\!].$$

And modulo n, we have

$$1 \equiv [\![a \mid n]\!]\,[\![a^{-1} \mid n]\!] \equiv a^{(n-1)/2}\,[\![a^{-1} \mid n]\!] \bmod n.$$

Which implies that $\left(a^{-1}\right)^{(n-1)/2} \equiv [\![a^{-1} \mid n]\!] \bmod n$. That is $a^{-1} \in J_n$.

Namely, J_n contains the identity, it is closed under inverse and multiplication, and it is now easy to verify that fulfill the other requirements to be a group. ■

Lemma 52.1.35. *Let n be an odd integer that is composite, then $|J_n| \leq \left|\mathbb{Z}_n^*\right|/2$.*

Proof: Let has the prime factorization $n = \prod_{i=1}^{t} p_i^{k_i}$. Let $q = p_1^{k_1}$, and $m = n/q$. By Lemma 52.1.20$_{\text{p7}}$, the group $\mathbb{Z}_q^*$ is cyclic, and let g be its generator. Consider the element $a \in \mathbb{Z}_n^*$ such that

$$a \equiv g \bmod q \qquad \text{and} \qquad a \equiv 1 \bmod m.$$

Such a number a exists and its unique, by the Chinese remainder theorem (Theorem 52.1.6$_{\text{p3}}$). In particular, let $m = \prod_{i=2}^{t} p_i^{k_i}$, and observe that, for all i, we have $a \equiv 1 \pmod{p_i}$, as $p_i \mid m$. As such, writing the Jacobi symbol explicitly, we have

$$[\![a \mid n]\!] = [\![a \mid q]\!] \prod_{i=2}^{t} (a \mid p_i)^{k_i} = [\![a \mid q]\!] \prod_{i=2}^{t} (1 \mid p_i)^{k_i} = [\![a \mid q]\!] \prod_{i=2}^{t} 1 = [\![a \mid q]\!] = [\![g \mid q]\!] .$$

since $a \equiv g \pmod q$, and Lemma 52.1.32$_{\text{p11}}$ (C). At this point there are two possibilities:

(A) If $k_1 = 1$, then $q = p_1$, and $[\![g \mid q]\!] = (g \mid q) = g^{(q-1)/2} \pmod q$. But g is a generator of $\mathbb{Z}_q^*$, and its order is $q - 1$. As such $g^{(q-1)/2} \equiv -1 \pmod q$, see Definition 52.1.23$_{\text{p8}}$. We conclude that $[\![a \mid n]\!] = -1$. If we assume that $J_n = \mathbb{Z}_n^*$, then $[\![a \mid n]\!] \equiv a^{(n-1)/2} \equiv -1 \pmod n$. Now, as $m \mid n$, we have

$$a^{(n-1)/2} \equiv_m \left(a^{(n-1)/2} \bmod n\right) \bmod m \equiv_m -1.$$

But this contradicts the choice of a as $a \equiv 1 \pmod m$.

(B) If $k_1 > 1$ then $q = p_1^{k_1}$. Arguing as above, we have that $[\![a \mid n]\!] = (-1)^{k_1}$. Thus, if we assume that $J_n = \mathbb{Z}_n^*$, then $a^{(n-1)/2} \equiv -1 \pmod n$ or $a^{(n-1)/2} \equiv 1 \pmod n$. This implies that $a^{n-1} \equiv 1 \pmod n$. Thus, $a^{n-1} \equiv 1 \pmod q$.

Now $a \equiv g \mod q$, and thus $g^{n-1} \equiv 1 \pmod q$. This implies that the order of g in $\mathbb{Z}_q^*$ must divide $n-1$. That is $\operatorname{ord}(g) = \phi(q) \mid n-1$. Now, since $k_1 \geq 2$, we have that $p_1 \mid \phi(q) = \left(p_1^{k_1}\right)(p_1 - 1)$, see Lemma 52.1.8$_{\text{p3}}$. We conclude that $p_1 \mid n-1$ and $p_1 \mid n$, which is of course impossible, as $p_1 > 1$.

We conclude that J_n must be a proper subgroup of $\mathbb{Z}_n^*$, but, by Lemma 52.1.11$_{\text{p5}}$, it must be that $|J_n| \mid |\mathbb{Z}_n^*|$. But this implies that $|J_n| \leq |\mathbb{Z}_n^*|/2$. ■

52.2. Primality testing

The primality test is now easy[3]. Indeed, given a number n, first check if it is even (duh!). Otherwise, randomly pick a number $r \in \{2, \ldots, n-1\}$. If $\gcd(r, n) > 1$ then the number is composite. Otherwise, check if $r \in J_n$ (see Eq. (52.2)$_{\text{p12}}$), by computing $x = [\![r \mid n]\!]$ in polynomial time, see Section 52.1.3.4$_{\text{p12}}$, and $x' = a^{(n-1)/2} \bmod n$. (see Lemma 52.1.7$_{\text{p3}}$). If $x = x'$ then the algorithm returns is prime, otherwise it returns it is composite.

Theorem 52.2.1. *Given a number n, and a parameter $\delta > 0$, there is a randomized algorithm that, decides if the given number is prime or composite. The running time of the algorithm is $O\big((\log n)^c \log(1/\delta)\big)$, where c is some constant. If the algorithm returns that n is composite then it is. If the algorithm returns that n is prime, then is wrong with probability at most δ.*

[3] One could even say "trivial" with heavy Russian accent.

Proof: Run the above algorithm $m = O(\log(1/\delta))$ times. If any of the runs returns that it is composite then the algorithm return that n is composite, otherwise the algorithms returns that it is a prime.

If the algorithm fails, then n is a composite, and let $r_1, \ldots, r_m$ be the random numbers the algorithm picked. The algorithm fails only if $r_1, \ldots, r_m \in J_n$, but since $|J_n| \leq \left|\mathbb{Z}_n^2\right|/2$, by Lemma 52.1.35$_{\text{p12}}$, it follows that this happens with probability at most $\left(|J_n| / \left|\mathbb{Z}_n^2\right|\right)^m \leq 1/2^m \leq \delta$, as claimed. ■

52.2.1. Distribution of primes

In the following, let $\pi(n)$ denote the number of primes between 1 and n. Here, we prove that $\pi(n) = \Theta(n/\log n)$.

Lemma 52.2.2. *Let Δ be the product of all the prime numbers p, where $m < p \leq 2m$. We have that $\Delta \leq \binom{2m}{m}$.*

Proof: Let X be the product of the all composite numbers between m and $2m$, we have

$$\binom{2m}{m} = \frac{2m \cdot (2m-1) \cdots (m+2) \cdot (m+1)}{m \cdot (m-1) \cdots 2 \cdot 1} = \frac{X \cdot \Delta}{m \cdot (m-1) \cdots 2 \cdot 1}.$$

Since none of the numbers between 2 and m divides any of the factors of Δ, it must be that the number $\frac{X}{m \cdot (m-1) \cdots 2 \cdot 1}$ is an integer number, as $\binom{2m}{m}$ is an integer. Therefore, $\binom{2m}{m} = c \cdot \Delta$, for some integer $c > 0$, implying the claim. ■

Lemma 52.2.3. *The number of prime numbers between m and $2m$ is $O(m/\ln m)$.*

Proof: Let us denote all primes between m and $2m$ as $p_1 < p_2 < \cdots < p_k$. Since $p_1 \geq m$, it follows from Lemma 52.2.2 that $m^k \leq \prod_{i=1}^k p_i \leq \binom{2m}{m} \leq 2^{2m}$. Now, taking log of both sides, we have $k \lg m \leq 2m$. Namely, $k \leq 2m/\lg m$. ■

Lemma 52.2.4. *$\pi(n) = O(n/\ln n)$.*

Proof: Let the number of primes less than n be $\Pi(n)$, then by Lemma 52.2.3, there exist some positive constant C, such that for all $\forall n \geq N$, we have $\Pi(2n) - \Pi(n) \leq C \cdot n/\ln n$. Namely, $\Pi(2n) \leq C \cdot n/\ln n + \Pi(n)$. Thus, $\Pi(2n) \leq \displaystyle\sum_{i=0}^{\lceil \lg n \rceil} \left(\Pi\left(2n/2^i\right) - \Pi\left(2n/2^{i+1}\right) \right) \leq \sum_{i=0}^{\lceil \lg n \rceil} C \cdot \frac{n/2^i}{\ln(n/2^i)} = O\left(\frac{n}{\ln n}\right)$, by observing that the summation behaves like a decreasing geometric series. ■

Lemma 52.2.5. *For integers m, k and a prime p, if $p^k \mid \binom{2m}{m}$, then $p^k \leq 2m$.*

Proof: Let $T(p, m)$ be the number of times p appear in the prime factorization of $m!$. Formally, $T(p, m)$ is the highest number k such that p^k divides $m!$. We claim that $T(p, m) = \sum_{i=1}^{\infty} \left\lfloor m/p^i \right\rfloor$. Indeed, consider an integer $\beta \leq m$, such that $\beta = p^t \gamma$, where γ is an integer that is not divisible by p. Observe that β contributes exactly to the first t terms of the summation of $T(p, m)$ – namely, its contribution to $m!$ as far as powers of p is counted correctly.

Let α be the maximum number such that p^α divides $\binom{2m}{m} = \frac{2m!}{m!m!}$. Clearly,

$$\alpha = T(p, 2m) - 2T(p, m) = \sum_{i=1}^{\infty} \left(\left\lfloor \frac{2m}{p^i} \right\rfloor - 2 \left\lfloor \frac{m}{p^i} \right\rfloor \right).$$

It is easy to verify that for any integers x, y, we have that $0 \leq \left\lfloor \frac{2x}{y} \right\rfloor - 2 \left\lfloor \frac{x}{y} \right\rfloor \leq 1$. In particular, let k be the largest number such that $\left(\left\lfloor \frac{2m}{p^k} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor \right) = 1$, and observe that $T(p, 2m) \leq k$ as only the proceedings $k-1$ terms might be non-zero in the summation of $T(p, 2m)$. But this implies that $\lfloor 2m/p^k \rfloor \geq 1$, which implies in turn that $p^k \leq 2m$, as desired. ■

Lemma 52.2.6. $\pi(n) = \Omega(n/\ln n)$.

Proof: Assume $\binom{2m}{m}$ have k prime factors, and thus can be written as $\binom{2m}{m} = \prod_{i=1}^{k} p_i^{n_i}$, By Lemma 52.2.5, we have $p_i^{n_i} \leq 2m$. Of course, the above product might not include some prime numbers between 1 and $2m$, and as such k is a lower bound on the number of primes in this range; that is, $k \leq \pi(2m)$. This implies $\dfrac{2^{2m}}{2m} \leq \dbinom{2m}{m} \leq \prod_{i=1}^{k} 2m = (2m)^k$. By taking lg of both sides, we have $\dfrac{2m - \lg(2m)}{\lg(2m)} \leq k \leq \pi(2m)$. ■

We summarize the result.

Theorem 52.2.7. *Let $\pi(n)$ be the number of distinct prime numbers between 1 and n. We have that $\pi(n) = \Theta(n/\ln n)$.*

52.3. Bibliographical notes

Miller [Mil76] presented the primality testing algorithm which runs in deterministic polynomial time but relies on Riemann's Hypothesis (which is still open). Later on, Rabin [Rab80] showed how to convert this algorithm to a randomized algorithm, without relying on the Riemann's hypothesis.

This write-up is based on various sources – starting with the description in [MR95], and then filling in some details from various sources on the web.

What is currently missing from the write-up is a description of the RSA encryption system. This would hopefully be added in the future. There are of course typos in these notes – let me know if you find any.

References

[Mil76] G. L. Miller. *Riemann's hypothesis and tests for primality. J. Comput. Sys. Sci.*, 13(3): 300–317, 1976.

[MR95] R. Motwani and P. Raghavan. *Randomized algorithms*. Cambridge, UK: Cambridge University Press, 1995.

[Rab80] M. O. Rabin. *Probabilistic algorithm for testing primality. J. Number Theory*, 12(1): 128–138, 1980.