The Legendre Symbol[a] and Quadratic Residuacity Test

- So $a^{(p-1)/2} \bmod p = \pm 1$ for $a \neq 0 \bmod p$.
- For odd prime p, define the **Legendre symbol** $(a \mid p)$ as

$$(a \mid p) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a } \textbf{quadratic nonresidue} \text{ modulo } p \end{cases}$$

- Euler's test implies $a^{(p-1)/2} = (a \mid p) \bmod p$ for any odd prime p and any integer a.
- Note that $(ab|p) = (a|p)(b|p)$.

[a] Andrien-Marie Legendre (1752–1833).

Gauss's Lemma

Lemma 64 (Gauss) *Let p and q be two odd primes. Then $(q|p) = (-1)^m$, where m is the number of residues in $R = \{iq \bmod p : 1 \leq i \leq (p-1)/2\}$ that are greater than $(p-1)/2$.*

- All residues in R are distinct.
  - If $iq = jq \bmod p$, then $p|(j-i)\,q$ or $p|q$.
- No two elements of R add up to p.
  - If $iq + jq = 0 \bmod p$, then $p|(i+j)$ or $p|q$.
- Consider the set R' of residues that result from R if we replace each of the m elements $a \in R$, where $a > (p-1)/2$, by $p - a$.

The Proof (concluded)

- All residues in R' are now at most $(p-1)/2$.
- In fact, $R' = \{1, 2, \ldots, (p-1)/2\}$.
  - Otherwise, two elements of R would add up to p.
- Alternatively, $R' = \{\pm iq \bmod p : 1 \leq i \leq (p-1)/2\}$, where exactly m of the elements have the minus sign.
- Taking the product of all elements in the two representations of R', we have $[(p-1)/2]! = (-1)^m q^{(p-1)/2}[(p-1)/2]! \bmod p$.
- Because $\gcd([(p-1)/2]!, p) = 1$, the lemma follows.

Legendre's Law of Quadratic Reciprocity

- Let p and q be two odd primes.
- Then their Legendre symbols are identical unless both numbers are 3 mod 4.

Lemma 65 (Gauss) $(p|q)(q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

- Sum the elements of R' in the previous proof in mod2.
- On one hand, this is just

$$\sum_{i=1}^{(p-1)/2} i = \frac{(p-1)(p+1)}{8} \bmod 2.$$

The Proof (continued)

- On the other hand, the sum equals

$$q \sum_{i=1}^{(p-1)/2} i - p \sum_{i=1}^{(p-1)/2} \lfloor \frac{iq}{p} \rfloor + mp \bmod 2.$$

  – Signs are irrelevant under mod2.

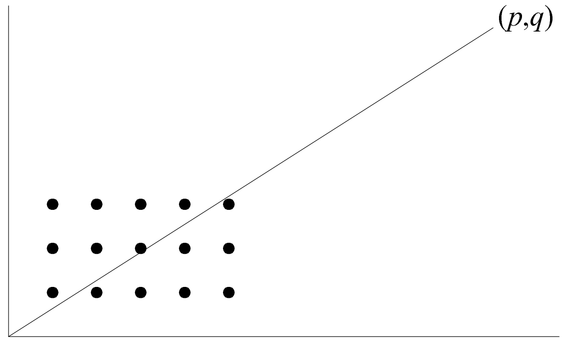
- After ignoring odd multipliers and noting that the first term above equals $\sum_{i=1}^{(p-1)/2} i$:

$$m = \sum_{i=1}^{(p-1)/2} \lfloor \frac{iq}{p} \rfloor \bmod 2.$$

The Proof (concluded)

- $m = \sum_{i=1}^{(p-1)/2} \lfloor \frac{iq}{p} \rfloor$ is the number of positive integral points in the $\frac{p-1}{2} \times \frac{q-1}{2}$ rectangle that are under the line between $(0,0)$ and the point (p,q).
- From Gauss's lemma on p. 379, $(q|p)$ is $(-1)^m$.
- Repeat the proof with p and q reversed.
- We obtain $(p|q)$ is -1 raised to the number of positive integral points in the $\frac{p-1}{2} \times \frac{q-1}{2}$ rectangle that are above the line between $(0,0)$ and the point (p,q).
- So $(p|q)(q|p)$ is -1 raised to the total number of integral points in the $\frac{p-1}{2} \times \frac{q-1}{2}$ rectangle, which is $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

Eisenstein's Rectangle



$p = 11$ and $q = 7$.

The Jacobi Symbol[a]

- The Legendre symbol only works for an odd *prime* modulus.
- The **Jacobi symbol** $(a \mid m)$ extends it to cases where m is not prime.
- Let $m = p_1 p_2 \cdots p_k$ be the prime factorization of m.
- When m is odd and is greater than one, then

$$(a|m) = \prod_{i=1}^{k} (a \mid p_i).$$

- Define $(a \mid 1) = 1$.

[a] Carl Jacobi (1804–1851).

Properties of the Jacobi Symbol

The Jacobi symbol has the following properties, for arguments for which it is defined.

1. $(ab \mid m) = (a \mid m)(b \mid m)$.
2. $(a \mid m_1 m_2) = (a \mid m_1)(a \mid m_2)$.
3. If $a = b \bmod m$, then $(a \mid m) = (b \mid m)$.
4. $(-1 \mid m) = (-1)^{(m-1)/2}$.
5. $(2 \mid m) = (-1)^{(m^2-1)/8}$.
6. If a and m are both odd, then $(a \mid m)(m \mid a) = (-1)^{(a-1)(m-1)/4}$.

Calculation of $(2200|999)$

Similar to the Euclidean algorithm and does *not* require factorization.

$$
\begin{aligned}
& (202|999) = (-1)^{(999^2-1)/8}(101|999) \\
= \; & (-1)^{124750}(101|999) = (101|999) \\
= \; & (-1)^{(100)(998)/4}(999|101) = (-1)^{24950}(999|101) \\
= \; & (999|101) = (90|101) = (-1)^{(101^2-1)/8}(45|101) \\
= \; & (-1)^{1275}(45|101) = -(45|101) \\
= \; & -(-1)^{(44)(100)/4}(101|45) = -(101|45) = -(11|45) \\
= \; & -(-1)^{(10)(44)/4}(45|11) = -(45|11) \\
= \; & -(1|11) = -(11|1) = -1.
\end{aligned}
$$

A Result Generalizing Proposition 10.3 in the Book

Theorem 66 *The group of set $\Phi(n)$ under multiplication* mod n *has a primitive root if and only if n is either 1, 2, 4, p^k, or $2p^k$ for some nonnegative integer k and and odd prime p.*

This result is essential in the proof of the next lemma.

The Jacobi Symbol and Primality Test[a]

Lemma 67 *If $(M|N) = M^{(N-1)/2} \bmod N$ for all $M \in \Phi(N)$, then N is prime. (Assume N is odd.)*

- Assume $N = mp$, where p is an odd prime, $\gcd(m, p) = 1$, and $m > 1$ (not necessarily prime).
- Let $r \in \Phi(p)$ such that $(r \mid p) = -1$.
- The Chinese remainder theorem says that there is an $M \in \Phi(N)$ such that

$$
\begin{aligned}
M &= r \bmod p \\
M &= 1 \bmod m
\end{aligned}
$$

[a] Clement Hsiao pointed out that the textbook's proof in Lemma 11.8 is incorrect while he was a senior in January 1999.

The Proof (continued)

- By the hypothesis,

$$M^{(N-1)/2} = (M \mid N) = (M \mid p)(M \mid m) = -1 \bmod N.$$

- Hence

$$M^{(N-1)/2} = -1 \bmod m.$$

- But because $M = 1 \bmod m$,

$$M^{(N-1)/2} = 1 \bmod m,$$

a contradiction.

The Proof (continued)

- Second, assume that $N = p^a$, where p is an odd prime and $a \geq 2$.
- By Theorem 66 (p. 388), there exists a primitive root r modulo p^a.
- From the assumption,

$$M^{N-1} = \left(M^{(N-1)/2}\right)^2 = (M|N)^2 = 1 \bmod N$$

for all $M \in \Phi(N)$.

The Proof (continued)

- As $r \in \Phi(N)$ (prove it), we have

$$r^{N-1} = 1 \bmod N.$$

- As r's exponent modulo $N = p^a$ is $\phi(N) = p^{a-1}(p-1)$,

$$p^{a-1}(p-1) \mid N-1,$$

which implies that $p \mid N-1$.

- But this is impossible given that $p \mid N$.

The Proof (continued)

- Third, assume that $N = mp^a$, where p is an odd prime, $\gcd(m, p) = 1$, $m > 1$ (not necessarily prime), and a is even.
- The proof mimics that of the second case.
- By Theorem 66 (p. 388), there exists a primitive root r modulo p^a.
- From the assumption,

$$M^{N-1} = \left(M^{(N-1)/2}\right)^2 = (M|N)^2 = 1 \bmod N$$

for all $M \in \Phi(N)$.

The Proof (continued)

- In particular,

$$M^{N-1} = 1 \bmod p^a \tag{6}$$

for all $M \in \Phi(N)$.

- The Chinese remainder theorem says that there is an $M \in \Phi(N)$ such that

$$\begin{aligned} M &= r \bmod p^a \\ M &= 1 \bmod m \end{aligned}$$

- Because $M = r \bmod p^a$ and Eq. (6),

$$r^{N-1} = 1 \bmod p^a.$$

The Proof (concluded)

- As r's exponent modulo $N = p^a$ is $\phi(N) = p^{a-1}(p-1)$,

$$p^{a-1}(p-1) \mid N-1,$$

which implies that $p \mid N-1$.

- But this is impossible given that $p \mid N$.

The Number of Witnesses to Compositeness

Theorem 68 (Solovay and Strassen, 1977) *If N is an odd composite, then $(M|N) \neq M^{(N-1)/2} \bmod N$ for at least half of $M \in \Phi(N)$.*

- By Lemma 67 there is at least one $a \in \Phi(N)$ such that $(a|N) \neq a^{(N-1)/2} \bmod N$.
- Let $B = \{b_1, b_2, \ldots, b_k\} \subseteq \Phi(N)$ be the set of all distinct residues such that $(b_i|N) = b_i^{(N-1)/2} \bmod N$.
- Let $aB = \{ab_i \bmod N : i = 1, 2, \ldots, k\}$

The Proof (concluded)

- $|aB| = k$.
  - $ab_i = ab_j \bmod N$ implies $N | a(b_i - b_j)$, which is impossible because $\gcd(a, N) = 1$ and $N > |b_i - b_j|$.
- $aB \cap B = \emptyset$ because

$$(ab_i)^{(N-1)/2} = a^{(N-1)/2} b_i^{(N-1)/2} \neq (a|N)(b_i|N) = (ab_i|N).$$

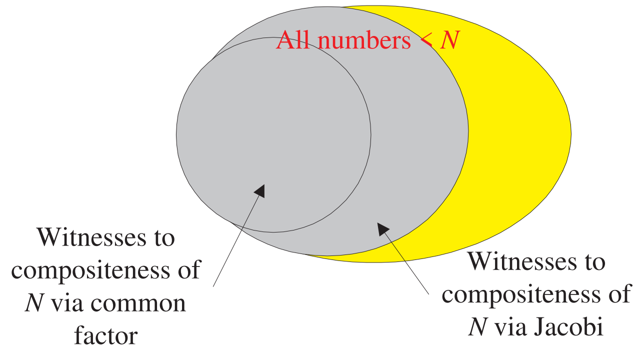
- Combining the above two results, we know $|B|/\phi(N) \leq 0.5$.

```
if N is even but N ≠ 2 then
  return "N is a composite";
else if N is even and N = 2 then
  return "N is a prime";
end if
Pick M ∈ {2, 3, ..., N − 1} randomly;
if gcd(M, N) > 1 then
  return "N is a composite";
else
  if (M|N) ≠ M^((N−1)/2) mod N then
    return "N is a composite";
  else
    return "N is probably a prime";
  end if
end if
```


Analysis

- The algorithm certainly runs in polynomial time.
- There are no false positives (for COMPOSITENESS).
  - When the algorithm says the number is a composite, it is always correct.
- The probability of a false negative is at most one half.
  - When the algorithm says the number is a prime, it may err.
  - If the input is a composite, then the probability that the algorithm errs is one half.
- The probability of error can be reduced but not eliminated.

The Improved Density Attack for PRIMES



Randomized Complexity Classes; RP

- Let N be a polynomial-time precise NTM that runs in time $p(n)$ and has 2 nondeterministic choices at each step.
- N is a **polynomial Monte Carlo Turing machine** for a language L if the following conditions hold:
  - If $x \in L$, then at least half of the $2^{p(|x|)}$ computation paths of N on x halt with "yes."
  - If $x \notin L$, then all computation paths halt with "no."
- The class of all languages with polynomial Monte Carlo TMs is denoted **RP** for **randomized polynomial time**.

Comments on RP

- Nondeterministic steps can be seen as fair coin flips.
- There are no false positive answers.
- The probability of false negatives is at most 0.5.
- Any constant $0 \leq \epsilon \leq 1$ can replace 0.5.
  - By repeating the algorithm k times, the probability of false negatives can be reduced to $(1-\epsilon)^k$.
  - Now pick $k = \lceil -\frac{1}{\log_2 1-\epsilon} \rceil$.
- In fact, ϵ can be arbitrarily close to 0 as long as it is of the order $1/p(n)$ for some polynomial $p(n)$.
  - $-\frac{1}{\log_2 1-\epsilon} = O(\frac{1}{\epsilon}) = O(p(n))$.

Where RP Fits

- $\mathrm{P} \subseteq \mathrm{RP} \subseteq \mathrm{NP}$.
  - A deterministic TM is like a Monte Carlo TM except that all the coin flips are ignored.
  - A Monte Carlo TM is an NTM with extra demands on the number of accepting paths.
- COMPOSITENESS $\in$ RP; PRIMES $\in$ coRP; PRIMES $\in$ RP.[a]
  - In fact, PRIMES $\in$ P.
- RP $\cup$ coRP is a "plausible" notion of efficient computation.

[a] Adleman and Huang, 1987.

ZPP[a] (Zero Probabilistic Polynomial)

- The class **ZPP** is defined as RP $\cap$ coRP.
- A language in ZPP has *two* Monte Carlo algorithms, one with no false positives and the other with no false negatives.
- If we repeatedly run both Monte Carlo algorithms, *eventually* one definite answer will come (unlike RP).
  - A *positive* answer from the one without false positives.
  - A *negative* answer from the one without false negatives.

[a] Gill, 1977.

The ZPP Algorithm (**Las Vegas**)

```
{Suppose L ∈ ZPP.}
{N1 has no false positives, and N2 has no false negatives.}
while true do
  if N1(x) = "yes" then
    return "yes";
  end if
  if N2(x) = "no" then
    return "no";
  end if
end while
```


ZPP (concluded)

- The *expected* running time for it to happen is polynomial.
  - The probability that a run of the 2 algorithms does not generate a definite answer is 0.5.
  - Let $p(n)$ be the running time of each run.
  - The expected running time for a definite answer is thus

$$\sum_{i=1}^{\infty} 0.5^i i p(n) = 2p(n).$$

You Too, RP?

```
{Suppose L ∈ RP.}
{N decides L without false positives.}
while true do
  if N(x) = "yes" then
    return "yes";
  end if
  {But what to do here?}
end while
```

- You eventually get a "yes" if $x \in L$.
- But how to get a "no" when $x \notin L$?

PP

- A language L is in the class **PP** if there is a polynomial-time precise NTM N such that:
  - For all inputs x, $x \in L$ if and only if more than half of the computations of N (i.e., $2^{p(n)-1} + 1$ or up) on input x end up with a "yes."
  - We say that N decides L by majority.
- MAJSAT: is it true that the majority of the 2^n truth assignments to ϕ's n variables satisfy it?
- MAJSAT is PP-complete.
- PP is closed under complement.

NP vs. PP

Theorem 69 *$NP \subseteq PP$.*

- Suppose $L \in$ NP is decided by an NTM N.
- Construct a new NTM N':
  - N' has one more extra state s than N.
  - N' starts at s and either branches to N's program or simply accepts (after $p(|\,x\,|)$ steps).
- Consider an input x.
- Suppose N on x computes for $p(|\,x\,|)$ steps and produces $2^{p(|\,x\,|)}$ computation paths.

The Proof (concluded)

- Then N' has $2^{p(|x|)+1}$ computation paths.
- Half of these will always halt with "yes."
- Thus a majority of the paths of N' accept x if and only if at least one path of N accepts x.
- That is, if and only if $x \in L$.
- So N' accepts L by majority and $L \in \text{PP}$.

Large Deviations

- You have a *biased* coin.
- One side has probability $0.5 + \epsilon$ to appear and the other $0.5 - \epsilon$, for some $0 < \epsilon < 1$.
- But you do not know which is which.
- How to decide which side is the more likely—with high confidence?
- Answer: Flip the coin many times and pick the side that appeared the most times.
- Question: Can you quantify the confidence?

The Chernoff Bound

Theorem 70 (Chernoff, 1952) *Suppose $x_1, x_2, \ldots, x_n$ are independent random variables taking the values 1 and 0 with probabilities p and $1-p$, respectively. Let $X = \sum_{i=1}^{n} x_i$. Then for all $0 \leq \theta \leq 1$,*

$$\text{prob}[\, X \geq (1+\theta)pn \,] \leq e^{-\theta^2 pn/3}.$$

- The probability that the deviate of a **binomial random variable** from its expected value decreases exponentially with the deviation.
- The Chernoff bound is asymptotically optimal.

The Proof

- Let t be any positive real number.
- Then
$$\text{prob}[\, X \geq (1+\theta)pn \,] = \text{prob}[\, e^{tX} \geq e^{t(1+\theta)pn} \,].$$
- Markov's inequality (p. 360) generalized to real-valued random variables says that
$$\text{prob}\left[\, e^{tX} \geq kE[\, e^{tX} \,] \,\right] \leq 1/k.$$
- With $k = e^{t(1+\theta)pn} / E[\, e^{tX} \,]$, we have
$$\text{prob}[\, X \geq (1+\theta)pn \,] \leq e^{-t(1+\theta)pn} E[\, e^{tX} \,].$$

The Proof (continued)

- Because $X = \sum_{i=1}^{n} x_i$ and x_i's are independent,

$$E[\, e^{tX} \,] = (E[\, e^{t x_1} \,])^n = [\, 1 + p(e^t - 1) \,]^n.$$

- Substituting, we obtain

$$\begin{aligned} \text{prob}[\, X \geq (1+\theta)pn \,] &\leq e^{-t(1+\theta)pn} [\, 1 + p(e^t - 1) \,]^n \\ &\leq e^{-t(1+\theta)pn} e^{pn(e^t - 1)} \end{aligned}$$

as $(1+a)^n \leq e^{an}$ for all $a > 0$.

The Proof (concluded)

- With the choice of $t = \ln(1+\theta)$, the above becomes

$$\text{prob}[\, X \geq (1+\theta)pn \,] \leq e^{pn[\, \theta - (1+\theta)\ln(1+\theta) \,]}.$$

- The exponent expands to $-\frac{\theta^2}{2} + \frac{\theta^3}{6} - \frac{\theta^4}{12} + \cdots$ for $0 \leq \theta \leq 1$, which is less than

$$-\frac{\theta^2}{2} + \frac{\theta^3}{6} \leq \theta^2 \left(-\frac{1}{2} + \frac{\theta}{6} \right) \leq \theta^2 \left(-\frac{1}{2} + \frac{1}{6} \right) = -\frac{\theta^2}{3}.$$

Effectiveness of the Majority Rule

From $\text{prob}[\, X \leq (1-\theta)pn \,] \leq e^{-\frac{\theta^2}{2} pn}$ (prove it):

Corollary 71 *If $p = (1/2) + \epsilon$ for some $0 \leq \epsilon \leq 1/2$, then*

$$\text{prob}\left[\sum_{i=1}^{n} x_i \leq n/2 \right] \leq e^{-\epsilon^2 n/2}.$$

- The textbook's corollary to Lemma 11.9 seems incorrect.
- Our original problem (p. 411) hence demands $\approx 1.4k/\epsilon^2$ independent coin flips to guarantee making an error with probability at most 2^{-k} with the majority rule.