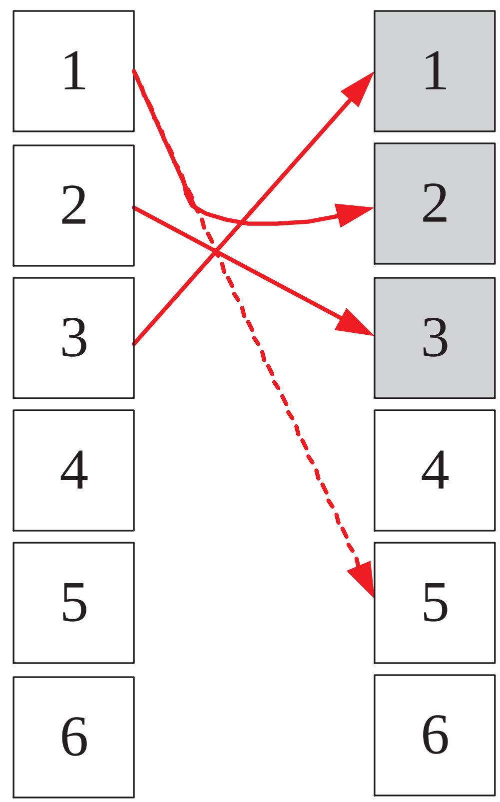
## Gauss's Lemma

**Lemma 63 (Gauss)** *Let $p$ and $q$ be two distinct 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 $p \,|\, (j-i)$ or $p|q$.
  - But neither is possible.
- No two elements of $R$ add up to $p$.
  - If $iq + jq = 0 \bmod p$, then $p|(i+j)$ or $p|q$.
  - But neither is possible.

## The Proof (continued)

- Replace each of the $m$ elements $a \in R$ such that $a > (p-1)/2$ by $p - a$.
  - This is equivalent to performing $-a \bmod p$.
- Call the resulting set of residues $R'$.
- All numbers in $R'$ are at most $(p-1)/2$.
- In fact, $R' = \{1, 2, \ldots, (p-1)/2\}$ (see illustration next page).
  - Otherwise, two elements of $R$ would add up to $p$, which has been shown to be impossible.




$p = 7$ and $q = 5$.

## The Proof (concluded)

- Alternatively, $R' = \{\pm iq \bmod p : 1 \leq i \leq (p-1)/2\}$, where exactly $m$ of the elements have the minus sign.
- Take the product of all elements in the two representations of $R'$.
- So

$$[(p-1)/2]! = (-1)^m q^{(p-1)/2} [(p-1)/2]! \bmod p.$$

- Because $\gcd([(p-1)/2]!, p) = 1$, the above implies

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

## Legendre's Law of Quadratic Reciprocity[a]

- Let $p$ and $q$ be two distinct odd primes.
- The next result says their Legendre symbols are distinct if and only if both numbers are 3 mod 4.

**Lemma 64 (Legendre (1785), Gauss)**

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

[a] First stated by Euler in 1751. Legendre (1785) did not give a correct proof. Gauss proved the theorem when he was 19. He gave at least 8 different proofs during his life. The 152nd proof appeared in 1963. A computer-generated formal proof was given in Russinoff (1990). As of 2008, there have been 4 such proofs. According to Wiedijk (2008), "the Law of Quadratic Reciprocity is the first nontrivial theorem that a student encounters in the mathematics curriculum."

## The Proof (continued)

- Sum the elements of $R'$ in the previous proof in mod2.
- On one hand, this is just $\sum_{i=1}^{(p-1)/2} i \bmod 2$.
- On the other hand, the sum equals

$$\begin{aligned} & mp + \sum_{i=1}^{(p-1)/2} \left( iq - p \left\lfloor \frac{iq}{p} \right\rfloor \right) \bmod 2 \\ = \quad & mp + \left( q \sum_{i=1}^{(p-1)/2} i - p \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{iq}{p} \right\rfloor \right) \bmod 2. \end{aligned}$$

  - $m$ of the $iq \bmod p$ are replaced by $p - iq \bmod p$.
  - But signs are irrelevant under mod2.
  - $m$ is as in Lemma 63 (p. 531).

## The Proof (continued)

- Ignore odd multipliers to make the sum equal

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

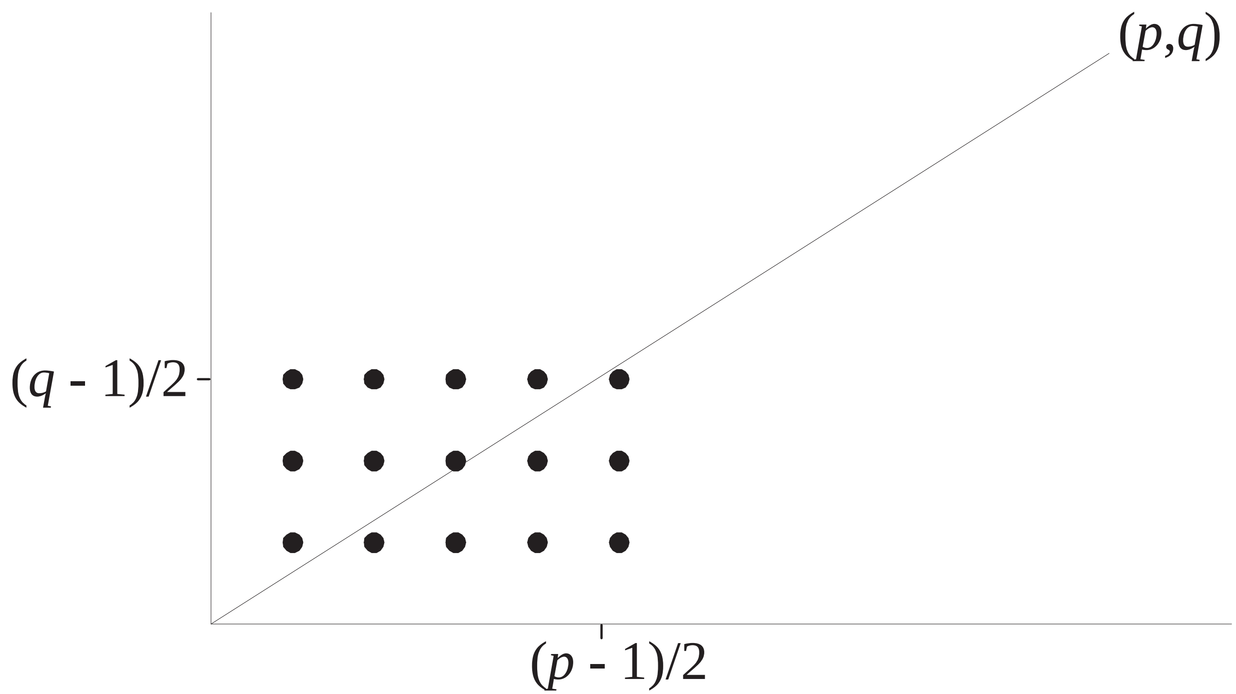
- Equate the above with $\sum_{i=1}^{(p-1)/2} i \bmod 2$ to obtain

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

# The Proof (concluded)

- $\sum_{i=1}^{(p-1)/2} \lfloor \frac{iq}{p} \rfloor$ is the number of integral points *below* the line
$$y = (q/p)\,x$$
for $1 \leq x \leq (p-1)/2$.
- Gauss's lemma (p. 531) says $(q|p) = (-1)^m$.
- Repeat the proof with $p$ and $q$ reversed.
- Then $(p|q) = (-1)^{m'}$, where $m'$ is the number of integral points *above* the line $y = (q/p)\,x$ for $1 \leq y \leq (q-1)/2$.
- As a result, $(p|q)(q|p) = (-1)^{m+m'}$.
- But $m + m'$ is the total number of integral points in the $[1, \frac{p-1}{2}] \times [1, \frac{q-1}{2}]$ rectangle, which is $\frac{p-1}{2} \frac{q-1}{2}$.

# Eisenstein's Rectangle




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

# The Jacobi Symbol[a]

- The Legendre symbol only works for odd *prime* moduli.
- 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 $m > 1$ is odd and $\gcd(a, m) = 1$, then

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

  - Note that the Jacobi symbol equals $\pm 1$.
  - It reduces to the Legendre symbol when $m$ is a prime.
- 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. $(ab \,|\, m) = (a \,|\, m)(b \,|\, m)$.
2. $(a \,|\, m_1 m_2) = (a \,|\, m_1)(a \,|\, m_2)$.
3. If $a = b \bmod m$, then $(a \,|\, m) = (b \,|\, m)$.
4. $(-1 \,|\, m) = (-1)^{(m-1)/2}$ (by Lemma 63 on p. 531).
5. $(2 \,|\, m) = (-1)^{(m^2-1)/8}$.[a]
6. If $a$ and $m$ are both odd, then $(a \,|\, m)(m \,|\, a) = (-1)^{(a-1)(m-1)/4}$.

---

[a] By Lemma 63 (p. 531) and some parity arguments.

## Properties of the Jacobi Symbol (concluded)

- These properties allow us to calculate the Jacobi symbol *without* factorization.
- This situation is similar to the Euclidean algorithm.
- Note also that $(a \,|\, m) = 1/(a \,|\, m)$ because $(a \,|\, m) = \pm 1$.[a]

---

[a]Contributed by Mr. Huang, Kuan-Lin (`B96902079`, `R00922018`) on December 6, 2011.

# Calculation of $(2200|999)$

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

# A Result Generalizing Proposition 10.3 in the Textbook

**Theorem 65** *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 66** *If* $(M|N) = M^{(N-1)/2} \bmod N$ *for all* $M \in \Phi(N)$*, then* $N$ *is a 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 $(r \,|\, p) = -1$.
- 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] Mr. Clement Hsiao (`B4506061`, `R88526067`) pointed out that the textbook's proof for Lemma 11.8 is incorrect in January 1999 while he was a senior.

## 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 65 (p. 544), 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 $\phi(N) = p^{a-1}(p-1)$,
$$p^{a-1}(p-1) \,|\, (N-1),$$
which implies that $p \,|\, (N-1)$.
- But this is impossible given that $p \,|\, N$.

## 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 65 (p. 544), 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,
$$M^{N-1} = 1 \bmod p^a \tag{13}$$
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. (13),
$$r^{N-1} = 1 \bmod p^a.$$

# The Proof (concluded)

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

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

  which implies that $p \,|\, (N-1)$.

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

## The Number of Witnesses to Compositeness

**Theorem 67 (Solovay and Strassen (1977))** *If $N$ is an odd composite, then $(M|N) = M^{(N-1)/2} \bmod N$ for at most half of $M \in \Phi(N)$.*

- By Lemma 66 (p. 545) 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 $aB = \{ab_i \bmod N : i = 1, 2, \ldots, k\}$.
- Clearly, $aB \subseteq \Phi(N)$, too.

## The Proof (concluded)

- $|aB| = k$.
  - $ab_i = ab_j \bmod N$ implies $N \mid a(b_i - b_j)$, 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

$$\frac{|\,B\,|}{\phi(N)} \leq \frac{|\,B\,|}{|\,B \cup aB\,|} = 0.5.$$

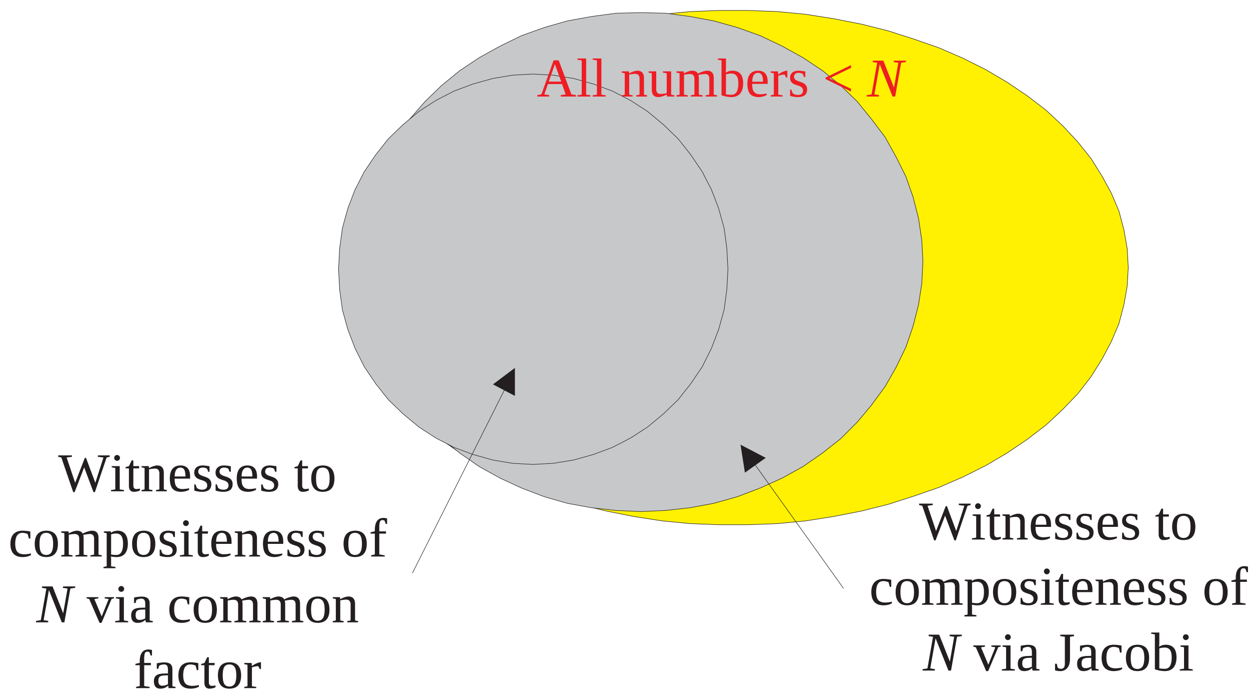
```
if N is even but N ≠ 2 then
    return "N is composite";
else if N = 2 then
    return "N is a prime";
end if
Pick M ∈ {2, 3, ..., N − 1} randomly;
if gcd(M, N) > 1 then
    return "N is composite";
else
    if (M|N) = M^((N−1)/2) mod N then
        return "N is (probably) a prime";
    else
        return "N is composite";
    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 composite, it is always correct.
- The probability of a false negative is at most one half.
  - Suppose the input is composite.
  - The probability that the algorithm says the number is a prime is $\leq 0.5$ by Theorem 67 (p. 552).
- So it is a Monte Carlo algorithm for COMPOSITENESS.

## The Improved Density Attack for COMPOSITENESS



## 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 $2^{p(n)}$ computation paths of $N$ on $x$ halt with "yes" where $n = |\, x \,|$.
  - If $x \notin L$, then all computation paths halt with "no."
- The class of all languages with polynomial Monte Carlo TMs is denoted **RP** (**randomized polynomial time**).[a]

[a] Adleman and Manders (1977).

## Comments on RP

- In analogy to Proposition 35 (p. 306), a "yes" instance of an RP problem has many certificates (witnesses).
- There are no false positives.
- If we associate nondeterministic steps with flipping fair coins, then we can cast RP in the language of probability.
  - If $x \in L$, then $N(x)$ halts with "yes" with probability at least 0.5 .
  - If $x \notin L$, then $N(x)$ halts with "no."

## Comments on RP (concluded)

- The probability of false negatives is $\epsilon \leq 0.5$.
- But *any* constant between 0 and 1 can replace 0.5.
  - Repeat the algorithm $k = \lceil -\frac{1}{\log_2 \epsilon} \rceil$ times and answer "yes" only if all runs answer "yes."
  - The probability of false negatives becomes $\epsilon^k \leq 0.5$.
- In fact, $\epsilon$ can be arbitrarily close to 1 as long as it is at most $1 - 1/q(n)$ for some polynomial $q(n)$.
  - $-\frac{1}{\log_2 \epsilon} = O(\frac{1}{1-\epsilon}) = O(q(n))$.

# Where RP Fits

- $P \subseteq RP \subseteq NP$.
  - 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;[a] PRIMES $\in$ coRP; PRIMES $\in$ RP.[b]
  - In fact, PRIMES $\in$ P.[c]
- RP $\cup$ coRP is an alternative "plausible" notion of efficient computation.

---

[a] Rabin (1976) and Solovay and Strassen (1977).
[b] Adleman and Huang (1987).
[c] Agrawal, Kayal, and Saxena (2002).

# ZPP[a] (Zero Probabilistic Polynomial)

- The class **ZPP** is defined as $\text{RP} \cap \text{coRP}$.
- 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.}
{N_1 has no false positives, and N_2 has no false
negatives.}
while true do
   if N_1(x) = "yes" then
      return "yes";
   end if
   if N_2(x) = "no" then
      return "no";
   end if
end while
```

# ZPP (concluded)

- The *expected* running time for the correct answer to emerge is polynomial.
  - The probability that a run of the 2 algorithms does not generate a definite answer is 0.5 (why?).
  - Let $p(n)$ be the running time of each run of the while-loop.
  - The expected running time for a definite answer is

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

- Essentially, ZPP is the class of problems that can be solved, without errors, in expected polynomial time.

# Large Deviations

- Suppose you have a *biased* coin.
- One side has probability $0.5 + \epsilon$ to appear and the other $0.5 - \epsilon$, for some $0 < \epsilon < 0.5$.
- But you do not know which is which.
- How to decide which side is the more likely side—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[a]

**Theorem 68 (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

  $$E[\, X \,] = E\left[ \sum_{i=1}^n x_i \right] = pn$$

  decreases exponentially with the deviation.

[a]Herman Chernoff (1923–). The 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. 503) 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,

$$E[\, e^{tX} \,] = (E[\, e^{tx_1} \,])^n = [\, 1 + p(e^t - 1) \,]^n.$$

- 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 $0 \leq \theta \leq 1$.
- But it is less than
$$-\frac{\theta^2}{2} + \frac{\theta^3}{6} \leq \theta^2 \left( -\frac{1}{2} + \frac{\theta}{6} \right) \leq \theta^2 \left( -\frac{1}{2} + \frac{1}{6} \right) = -\frac{\theta^2}{3}.$$

## Power of the Majority Rule

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

**Corollary 69** *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.[a]
- Our original problem (p. 564) hence demands, e.g., $n \approx 1.4k/\epsilon^2$ independent coin flips to guarantee making an error with probability $\leq 2^{-k}$ with the majority rule.

[a]See Dubhashi and Panconesi (2012) for many Chernoff-type bounds.

## BPP[a] (Bounded Probabilistic Polynomial)

- The class **BPP** contains all languages $L$ for which there is a precise polynomial-time NTM $N$ such that:
  - If $x \in L$, then at least $3/4$ of the computation paths of $N$ on $x$ lead to "yes."
  - If $x \notin L$, then at least $3/4$ of the computation paths of $N$ on $x$ lead to "no."
- So $N$ accepts or rejects by a *clear* majority.

[a] Gill (1977).

# Magic 3/4?

- The number 3/4 bounds the probability (ratio) of a right answer away from 1/2.
- Any constant *strictly* between 1/2 and 1 can be used without affecting the class BPP.
- In fact, as with RP,

$$\frac{1}{2} + \frac{1}{q(n)}$$

  for any polynomial $q(n)$ can replace 3/4 (p. 559).
- The next algorithm shows why.

# The Majority Vote Algorithm

Suppose $L$ is decided by $N$ by majority $(1/2) + \epsilon$.

**for** $i = 1, 2, \ldots, 2k + 1$ **do**
    Run $N$ on input $x$;
**end for**
**if** "yes" is the majority answer **then**
    "yes";
**else**
    "no";
**end if**

# Analysis

- The running time remains polynomial: $2k+1$ times $N$'s running time.
- By Corollary 69 (p. 569), the probability of a false answer is at most $e^{-\epsilon^2 k}$.
- By taking $k = \lceil 2/\epsilon^2 \rceil$, the error probability is at most $1/4$.
- Recall that $\epsilon$ can be any inverse polynomial.
- So $k$ remains a polynomial in $n$.

# Aspects of BPP

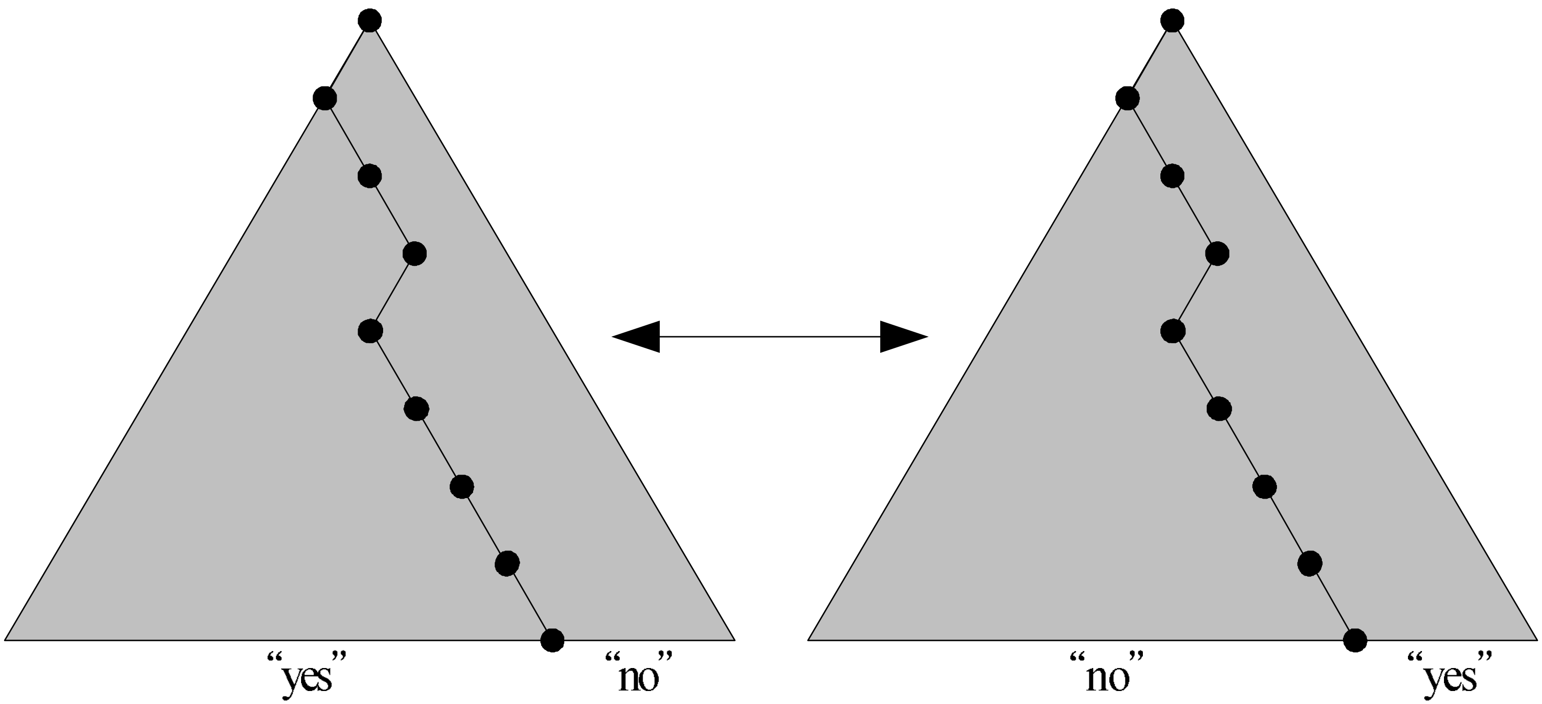
- BPP is the most comprehensive yet plausible notion of efficient computation.
  - If a problem is in BPP, we take it to mean that the problem can be solved efficiently.
  - In this aspect, BPP has effectively replaced P.
- $(\text{RP} \cup \text{coRP}) \subseteq (\text{NP} \cup \text{coNP})$.
- $(\text{RP} \cup \text{coRP}) \subseteq \text{BPP}$.
- Whether $\text{BPP} \subseteq (\text{NP} \cup \text{coNP})$ is unknown.
- But it is unlikely that $\text{NP} \subseteq \text{BPP}$ (see p. 591 and p. 592).

# coBPP

- The definition of BPP is symmetric: acceptance by clear majority and rejection by clear majority.
- An algorithm for $L \in$ BPP becomes one for $\bar{L}$ by reversing the answer.
- So $\bar{L} \in$ BPP and BPP $\subseteq$ coBPP.
- Similarly coBPP $\subseteq$ BPP.
- Hence BPP $=$ coBPP.
- This approach does not work for RP.[a]

[a] It did not work for NP either.

# BPP and coBPP



# BPP and P

**Theorem 70 (Nisan and Wigderson (1994))** *If every language in BPP only needs a pseudorandom generator which stretches a random seed of logarithmic length, then BPP = P.*

- We only need to show BPP $\subseteq$ P.
- Run the BPP algorithm for each of the seeds.
  - There are only $2^{O(\log n)} = O(n^c)$ seeds, a polynomial
- Accept if and only if at least $3/4$ of the outcomes is a "yes."
- The running time is clearly deterministically polynomial.

## "The Good, the Bad, and the Ugly"