Factorization and Primality Testing Chapter 6 Primality and Probability

Robert C. Vaughan

October 25, 2024

Miller-Rabin

- In its simplest form the Miller-Rabin test is a test for composites, although with some compromises it is also an effective test for primality.

Miller-Rabin

- In its simplest form the Miller-Rabin test is a test for composites, although with some compromises it is also an effective test for primality.
- The basic question is how easy is it to find a witness a in the following theorem when n is composite and how easy is it to determine that there is no witness when n is prime?

Theorem 1

Let $n \in \mathbb{N}$ be odd, $n > 1$ and take out the powers of 2 from $n-1$ so that

$$n - 1 = 2^u v$$

where v is odd. Choose $a \in \{2, 3, \dots, n-2\}$. If

$$a^v \not\equiv 1 \pmod{n} \text{ and } a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u-1, \tag{1.1}$$

then n is composite and a is a **witness**.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \dots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u - 1,$$

then n is composite and a is a **witness**.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u - 1,$$

then n is composite and a is a **witness**.

- **Proof.** The proof of the theorem is quite simple.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u - 1,$$

then n is composite and a is a **witness**.

- **Proof.** The proof of the theorem is quite simple.
- If $(a, n) > 1$, then (1.1) will hold and n will be composite. Suppose that $(a, n) = 1$ and n were to be prime. Then by Fermat-Euler we have $n | a^{n-1} - 1 =$

$$a^{2^u v} - 1 = (a^v - 1)(a^v + 1)(a^{2v} + 1)\ldots(a^{2^{u-1}v} + 1) \quad (1.2)$$

and n would have to divide one of the factors on the right, contradicting the hypothesis.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u - 1,$$

then n is composite and a is a **witness**.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u-1,$$

then n is composite and a is a **witness**.

- We would like to make this theorem the basis for an algorithm.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u - 1,$$

  then n is composite and a is a **witness**.
- We would like to make this theorem the basis for an algorithm.
- It is useful to eliminate some easily checked possibilities.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u - 1,$$

  then n is composite and a is a **witness**.
- We would like to make this theorem the basis for an algorithm.
- It is useful to eliminate some easily checked possibilities.
- A. Check n for small prime factors p for, say, $p \le \log n$.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \le w \le u - 1,$$

then n is composite and a is a **witness**.
- We would like to make this theorem the basis for an algorithm.
- It is useful to eliminate some easily checked possibilities.
- A. Check n for small prime factors p for, say, $p \le \log n$.
- B. Check that n is not a prime power, $n = p^k$. One can do this by checking to see if

$$n^{1/k} = \lfloor n^{1/k} \rfloor$$

for $2 \le k \le \frac{\log n}{\log 2}$.

- **Theorem 1.** Let $2 \nmid n \in \mathbb{N}$, $n > 1$ and suppose $n - 1 = 2^u v$ and $2 \nmid v$. Choose $a \in \{2, 3, \ldots, n-2\}$. If $a^v \not\equiv 1 \pmod{n}$ and

$$a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \leq w \leq u - 1,$$

then n is composite and a is a **witness**.
- We would like to make this theorem the basis for an algorithm.
- It is useful to eliminate some easily checked possibilities.
- A. Check n for small prime factors p for, say, $p \leq \log n$.
- B. Check that n is not a prime power, $n = p^k$. One can do this by checking to see if

$$n^{1/k} = \lfloor n^{1/k} \rfloor$$

for $2 \leq k \leq \frac{\log n}{\log 2}$.
- Now if n is composite it will have to have two different prime factors.

- The next theorem tells us what is happening when n has at least two different prime factors.

Theorem 2

If n is odd and has at least two different prime factors p and q, then they can be chosen so that

$$p-1=2^j l,\ q-1=2^k m, j\le k,$$

and then there are a with $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$$

and such an a is a witness.

- The next theorem tells us what is happening when n has at least two different prime factors.

Theorem 2

If n is odd and has at least two different prime factors p and q, then they can be chosen so that

$$p-1=2^j l,\ q-1=2^k m, j\le k,$$

and then there are a with $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$$

and such an a is a witness.

- In other words in this case witnesses to compositeness certainly exist.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that

$$p-1=2^j l,\ q-1=2^k m, j\le k,$$

and then there are a with $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$$

and such an a is a witness.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that

$$p-1 = 2^j l,\ q-1 = 2^k m, j \le k,$$

and then there are a with $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right) > 0$$

and such an a is a witness.

- As it stands this theorem only proves the existence of witnesses.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that

$$p - 1 = 2^j l,\ q - 1 = 2^k m, j \le k,$$

and then there are a with $(a, n) = 1$ and

$$\left(1 + \left(\frac{a}{p}\right)_L\right)\left(1 - \left(\frac{a}{q}\right)_L\right) > 0$$

and such an a is a witness.

- As it stands this theorem only proves the existence of witnesses.
- Since we do not expect to have found numerical values for p or q, it does not tell us how to find the a.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that

$$p - 1 = 2^j l,\ q - 1 = 2^k m, j \le k,$$

and then there are a with $(a, n) = 1$ and

$$\left(1 + \left(\frac{a}{p}\right)_L\right)\left(1 - \left(\frac{a}{q}\right)_L\right) > 0$$

and such an a is a witness.

- As it stands this theorem only proves the existence of witnesses.
- Since we do not expect to have found numerical values for p or q, it does not tell us how to find the a.
- However it can be used to show that we do not have to search very far.

- Consider: a is a witness when $(a, n) = 1$ and

$$\left(1 + \left(\frac{a}{p}\right)_L\right)\left(1 - \left(\frac{a}{q}\right)_L\right) > 0.$$

- Consider: a is a witness when $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0.$$

- When $(a,n)=1$, $\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)$ is 0 or 1, and when it is 1, a is a witness.

- Consider: a is a witness when $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0.$$

- When $(a,n)=1$, $\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)$ is 0 or 1, and when it is 1, a is a witness.
- Thus the number of witnesses for n is at least

$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right).$$

- Consider: a is a witness when $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0.$$

- When $(a,n)=1$, $\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)$ is 0 or 1, and when it is 1, a is a witness.
- Thus the number of witnesses for n is at least

$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right).$$

- It is easily shown that

$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{p}\right)_L=\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{q}\right)_L=\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{pq}\right)_J=0.$$

- Consider: a is a witness when $(a,n)=1$ and
$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0.$$
- When $(a,n)=1$, $\frac14\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)$ is 0 or 1, and when it is 1, a is a witness.
- Thus the number of witnesses for n is at least
$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\frac14\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right).$$
- It is easily shown that
$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{p}\right)_L=\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{q}\right)_L=\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{pq}\right)_J=0.$$
- Hence $\displaystyle\sum_{\substack{a=1\\(a,n)=1}}^{n}\frac14\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)=\frac{\phi(n)}{4}.$

- Hence

$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right) = \frac{\phi(n)}{4}.$$

- Hence

$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right) = \frac{\phi(n)}{4}.$$

- Therefore at least a quarter of all reduced residues modulo n act as witness.

- Hence

$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right) = \frac{\phi(n)}{4}.$$

- Therefore at least a quarter of all reduced residues modulo n act as witness.
- Hence we can proceed by picking N values of a at random.

- Hence

$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right) = \frac{\phi(n)}{4}.$$

- Therefore at least a quarter of all reduced residues modulo n act as witness.
- Hence we can proceed by picking N values of a at random.
- Then the probability that none of them are witnesses is at most $(3/4)^N$.

- Hence
$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right) = \frac{\phi(n)}{4}.$$
- Therefore at least a quarter of all reduced residues modulo n act as witness.
- Hence we can proceed by picking N values of a at random.
- Then the probability that none of them are witnesses is at most $(3/4)^N$.
- Therefore if we pick, say, at least $10\log n$ numbers a at random, then we can be practically certain of finding a witness.

- If we want some kind of absolute certainty, then we can assume the truth of the Riemann hypothesis for the three functions $L(s;\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}$ with

$$\chi(m) = \left(\frac{m}{p}\right)_L, \chi(m) = \left(\frac{m}{q}\right)_L, \chi(m) = \left(\frac{m}{pq}\right)_J,$$

which means that we have to assume it for every Jacobi symbol modulo n since we do not know the values of p and q.

- If we want some kind of absolute certainty, then we can assume the truth of the Riemann hypothesis for the three functions $L(s;\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}$ with

$$\chi(m) = \left(\frac{m}{p}\right)_L, \chi(m) = \left(\frac{m}{q}\right)_L, \chi(m) = \left(\frac{m}{pq}\right)_J,$$

which means that we have to assume it for every Jacobi symbol modulo n since we do not know the values of p and q.
- This hypothesis implies that for $N = 2(\log n)^2$ we have

$$\sum_{\substack{r \le N \\ r \text{ prime}}} \left(1 - \frac{r}{N}\right)\left(1 + \left(\frac{r}{p}\right)_L\right)\left(1 - \left(\frac{r}{q}\right)_L\right)\log r > 0.$$

- If we want some kind of absolute certainty, then we can assume the truth of the Riemann hypothesis for the three functions $L(s;\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}$ with

$$\chi(m) = \left(\frac{m}{p}\right)_L, \chi(m) = \left(\frac{m}{q}\right)_L, \chi(m) = \left(\frac{m}{pq}\right)_J,$$

  which means that we have to assume it for every Jacobi symbol modulo n since we do not know the values of p and q.
- This hypothesis implies that for $N = 2(\log n)^2$ we have

$$\sum_{\substack{r \le N \\ r \text{ prime}}} \left(1 - \frac{r}{N}\right) \left(1 + \left(\frac{r}{p}\right)_L\right) \left(1 - \left(\frac{r}{q}\right)_L\right) \log r > 0.$$

- In turn, this tells us that not only is there a witness $a \le 2(\log n)^2$, but we can suppose that it is prime.

- If we want some kind of absolute certainty, then we can assume the truth of the Riemann hypothesis for the three functions $L(s;\chi)=\sum_{m=1}^{\infty}\frac{\chi(m)}{m^s}$ with

$$\chi(m)=\left(\frac{m}{p}\right)_L,\ \chi(m)=\left(\frac{m}{q}\right)_L,\ \chi(m)=\left(\frac{m}{pq}\right)_J,$$

which means that we have to assume it for every Jacobi symbol modulo n since we do not know the values of p and q.
- This hypothesis implies that for $N=2(\log n)^2$ we have

$$\sum_{\substack{r\le N\\ r \text{ prime}}}\left(1-\frac{r}{N}\right)\left(1+\left(\frac{r}{p}\right)_L\right)\left(1-\left(\frac{r}{q}\right)_L\right)\log r>0.$$

- In turn, this tells us that not only is there a witness $a\le 2(\log n)^2$, but we can suppose that it is prime.
- There is even some belief that one does not have to search beyond $C(\log n)\log\log n$.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that $p-1=2^jl$, $q-1=2^km, j\le k$, and then there are a with $(a,n)=1$ and $\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$ and such an a is a witness.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that $p-1=2^j l$, $q-1=2^k m, j \le k$, and then there are a with $(a,n)=1$ and $\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$ and such an a is a witness.
- **Proof.** Let p,q be as given. Choose a QR x modulo p and a QNR y modulo q. Then by the Chinese Remainder Theorem there are a with $a\equiv x \pmod p$, $\equiv y \pmod q$ and $(a,n)=1$ so that a satisfies the hypothesis.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that $p-1=2^jl$, $q-1=2^km, j\le k$, and then there are a with $(a,n)=1$ and $\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$ and such an a is a witness.
- **Proof.** Let p,q be as given. Choose a QR x modulo p and a QNR y modulo q. Then by the Chinese Remainder Theorem there are a with $a\equiv x \pmod p$, $\equiv y \pmod q$ and $(a,n)=1$ so that a satisfies the hypothesis.
- We need to show that it is a witness. Recall from Theorem 1 that u and v are given by $n-1=2^uv$ where v is odd. We need to show that $a^v\not\equiv 1 \pmod n$ and

$$a^{2^wv}\not\equiv -1 \pmod n \text{ for } 1\le w\le u-1.$$

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that $p-1=2^j l$, $q-1=2^k m, j\le k$, and then there are a with $(a,n)=1$ and $\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$ and such an a is a witness.
- **Proof.** Let p, q be as given. Choose a QR x modulo p and a QNR y modulo q. Then by the Chinese Remainder Theorem there are a with $a\equiv x \pmod p$, $\equiv y \pmod q$ and $(a,n)=1$ so that a satisfies the hypothesis.
- We need to show that it is a witness. Recall from Theorem 1 that u and v are given by $n-1=2^u v$ where v is odd. We need to show that $a^v\not\equiv 1 \pmod n$ and

$$a^{2^w v}\not\equiv -1 \pmod n \text{ for } 1\le w\le u-1.$$

- If $a^{n-1}\not\equiv 1 \pmod n$, then no factor on the right of

$$a^{n-1}-1=a^{2^u v}-1=(a^v-1)(a^v+1)(a^{2v}+1)\dots(a^{2^{u-1}v}+1)$$

can be divisible by n, which suffices.

- **Theorem 2.** If n is odd and has at least two different prime factors p and q, then they can be chosen so that $p-1=2^j l$, $q-1=2^k m, j\le k$, and then there are a with $(a,n)=1$ and $\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$ and such an a is a witness.
- **Proof.** Let p,q be as given. Choose a QR x modulo p and a QNR y modulo q. Then by the Chinese Remainder Theorem there are a with $a\equiv x \pmod p$, $\equiv y \pmod q$ and $(a,n)=1$ so that a satisfies the hypothesis.
- We need to show that it is a witness. Recall from Theorem 1 that u and v are given by $n-1=2^u v$ where v is odd. We need to show that $a^v\not\equiv 1 \pmod n$ and

$$a^{2^w v}\not\equiv -1 \pmod n \text{ for } 1\le w\le u-1.$$

- If $a^{n-1}\not\equiv 1 \pmod n$, then no factor on the right of

$$a^{n-1}-1=a^{2^u v}-1=(a^v-1)(a^v+1)(a^{2v}+1)\dots(a^{2^{u-1}v}+1)$$

can be divisible by n, which suffices.
- Thus we can suppose that we have $a^{n-1}\equiv 1 \pmod n$.

- Recall $n-1 = 2^u v$ where v is odd, $a^{n-1} \equiv 1 \pmod{n}$ and

$$a^{n-1} - 1 = a^{2^u v} - 1 = (a^v - 1)(a^v + 1)(a^{2v} + 1) \ldots (a^{2^{u-1}v} + 1)$$

- Recall $n-1=2^u v$ where v is odd, $a^{n-1}\equiv 1 \pmod{n}$ and

$$a^{n-1}-1=a^{2^u v}-1=(a^v-1)(a^v+1)(a^{2v}+1)\dots(a^{2^{u-1}v}+1)$$

- For $0\le w\le u-1$ we have

$$a^{2^w v}+1=(a^v-1+1)^{2^v}+1\equiv 2 \pmod{(a^v-1)}.$$

- Recall $n-1=2^u v$ where v is odd, $a^{n-1}\equiv 1 \pmod{n}$ and

$$a^{n-1}-1=a^{2^u v}-1=(a^v-1)(a^v+1)(a^{2v}+1)\dots(a^{2^{u-1}v}+1)$$

- For $0\le w\le u-1$ we have

$$a^{2^w v}+1=(a^v-1+1)^{2^v}+1\equiv 2 \pmod{(a^v-1)}.$$

- Hence $\left(a^v-1, a^{2^w v}+1\right)|2$.

- Recall $n-1 = 2^u v$ where v is odd, $a^{n-1} \equiv 1 \pmod{n}$ and

$$a^{n-1}-1 = a^{2^u v}-1 = (a^v-1)(a^v+1)(a^{2v}+1)\dots(a^{2^{u-1}v}+1)$$

- For $0 \le w \le u-1$ we have

$$a^{2^w v} + 1 = (a^v - 1 + 1)^{2^v} + 1 \equiv 2 \pmod{(a^v - 1)}.$$

- Hence $\left(a^v - 1, a^{2^w v} + 1\right)|2$.
- Likewise when $0 \le w < x \le u-1$

$$\begin{aligned} a^{2^x v} + 1 &= (a^{2^w v} + 1 - 1)^{2^{x-w}} + 1 \\ &\equiv (-1)^{2^{x-w}} + 1 \equiv 2 \pmod{a^{2^w v} + 1} \end{aligned}$$

- Recall $n-1 = 2^u v$ where v is odd, $a^{n-1} \equiv 1 \pmod{n}$ and

$$a^{n-1}-1 = a^{2^u v}-1 = (a^v-1)(a^v+1)(a^{2v}+1)\dots(a^{2^{u-1}v}+1)$$

- For $0 \le w \le u-1$ we have

$$a^{2^w v} + 1 = (a^v - 1 + 1)^{2^v} + 1 \equiv 2 \pmod{(a^v - 1)}.$$

- Hence $\left(a^v - 1, a^{2^w v} + 1\right)|2$.
- Likewise when $0 \le w < x \le u-1$

$$\begin{aligned} a^{2^x v} + 1 &= (a^{2^w v} + 1 - 1)^{2^{x-w}} + 1 \\ &\equiv (-1)^{2^{x-w}} + 1 \equiv 2 \pmod{a^{2^w v} + 1} \end{aligned}$$

- Therefore $\left(a^{2^w v} + 1, a^{2^x v} + 1\right)|2$.

- Recall $n-1 = 2^u v$ where v is odd, $a^{n-1} \equiv 1 \pmod{n}$ and

$$a^{n-1}-1 = a^{2^u v}-1 = (a^v-1)(a^v+1)(a^{2v}+1)\dots(a^{2^{u-1}v}+1)$$

- For $0 \le w \le u-1$ we have

$$a^{2^w v} + 1 = (a^v - 1 + 1)^{2^v} + 1 \equiv 2 \pmod{(a^v - 1)}.$$

- Hence $\left(a^v - 1, a^{2^w v} + 1\right)|2$.
- Likewise when $0 \le w < x \le u-1$

$$a^{2^x v} + 1 = (a^{2^w v} + 1 - 1)^{2^{x-w}} + 1$$
$$\equiv (-1)^{2^{x-w}} + 1 \equiv 2 \pmod{a^{2^w v} + 1}$$

- Therefore $\left(a^{2^w v} + 1, a^{2^x v} + 1\right)|2$.
- Thus p and q, and *a fortiori* n, cannot divide two factors of $(a^v - 1)(a^v + 1)(a^{2v} + 1)\dots(a^{2^{u-1}v} + 1)$ and so it remains to consider the case when it divides exactly one.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.
- Let $e = \text{ord}_p(a)$ and $f = \text{ord}_q(a)$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, $a^{\frac{q-1}{2}} \equiv -1 \pmod q$.
- Let $e = \operatorname{ord}_p(a)$ and $f = \operatorname{ord}_q(a)$.
- Then $e \Big| \frac{p-1}{2} = 2^{j-1}l, f|q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, $a^{\frac{q-1}{2}} \equiv -1 \pmod q$.
- Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$.
- Then $e \left| \frac{p-1}{2} \right. = 2^{j-1} l, f | q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l' | l$, $m' | m$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.
- Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$.
- Then $e \Big| \frac{p-1}{2} = 2^{j-1}l, f|q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l'|l$, $m'|m$.
- In particular $0 \le i < j \le k$ (*).

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, $a^{\frac{q-1}{2}} \equiv -1 \pmod q$.
- Let $e = \operatorname{ord}_p(a)$ and $f = \operatorname{ord}_q(a)$.
- Then $e \left| \frac{p-1}{2} \right. = 2^{j-1}l, f|q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l'|l$, $m'|m$.
- In particular $0 \le i < j \le k$ (*).
- Recall that we are supposing that n divides exactly one of $a^v - 1, a^v + 1, \ldots, a^{2^{u-1}v} + 1$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, $a^{\frac{q-1}{2}} \equiv -1 \pmod q$.
- Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$.
- Then $e \left| \frac{p-1}{2} = 2^{j-1} l, f | q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k \right.$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l' | l$, $m' | m$.
- In particular $0 \le i < j \le k$ (*).
- Recall that we are supposing that n divides exactly one of $a^v - 1, a^v + 1, \ldots, a^{2^{u-1} v} + 1$.
- If $n | a^v - 1$, then $a^v \equiv 1 \pmod q$ and $f | v$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, $a^{\frac{q-1}{2}} \equiv -1 \pmod q$.
- Let $e = \text{ord}_p(a)$ and $f = \text{ord}_q(a)$.
- Then $e \Big| \frac{p-1}{2} = 2^{j-1}l, f|q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l'|l$, $m'|m$.
- In particular $0 \le i < j \le k$ (*).
- Recall that we are supposing that n divides exactly one of $a^v - 1,\ a^v + 1, \ldots, a^{2^{u-1}v} + 1$.
- If $n|a^v - 1$, then $a^v \equiv 1 \pmod q$ and $f|v$.
- But f is even and v is odd, so this is impossible.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.
- Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$.
- Then $e \left| \frac{p-1}{2} \right. = 2^{j-1}l, f | q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l' | l$, $m' | m$.
- In particular $0 \le i < j \le k$ (*).
- Recall that we are supposing that n divides exactly one of $a^v - 1, a^v + 1, \ldots, a^{2^{u-1}v} + 1$.
- If $n | a^v - 1$, then $a^v \equiv 1 \pmod{q}$ and $f | v$.
- But f is even and v is odd, so this is impossible.
- If $n | a^{2^s v} + 1$ for some s with $0 \le s \le u-1$, then $a^{2^{s+1}v} \equiv 1 \pmod{n}$, $a^{2^s v} \equiv -1 \pmod{n}$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.
- Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$.
- Then $e \Big| \frac{p-1}{2} = 2^{j-1}l, f|q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l'|l$, $m'|m$.
- In particular $0 \le i < j \le k$ (*).
- Recall that we are supposing that n divides exactly one of $a^v - 1,\ a^v + 1, \ldots, a^{2^{u-1}v} + 1$.
- If $n|a^v - 1$, then $a^v \equiv 1 \pmod{q}$ and $f|v$.
- But f is even and v is odd, so this is impossible.
- If $n|a^{2^s v} + 1$ for some s with $0 \le s \le u-1$, then $a^{2^{s+1}v} \equiv 1 \pmod{n}$, $a^{2^s v} \equiv -1 \pmod{n}$.
- Thus $e|2^{s+1}v$, $e \nmid 2^s v$, $e = 2^i l'$, $l'|v, i = s+1$ and $f|2^{s+1}v$, $f = 2^k m'$, $2^k m'|2^{s+1}v$, $m'|v$, $k \le s+1$.

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.
- Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$.
- Then $e \,\Big|\, \frac{p-1}{2} = 2^{j-1}l, f|q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l'|l$, $m'|m$.
- In particular $0 \le i < j \le k$ (*).
- Recall that we are supposing that n divides exactly one of $a^v - 1, a^v + 1, \ldots, a^{2^{u-1}v} + 1$.
- If $n|a^v - 1$, then $a^v \equiv 1 \pmod{q}$ and $f|v$.
- But f is even and v is odd, so this is impossible.
- If $n|a^{2^s v} + 1$ for some s with $0 \le s \le u-1$, then $a^{2^{s+1}v} \equiv 1 \pmod{n}$, $a^{2^s v} \equiv -1 \pmod{n}$.
- Thus $e|2^{s+1}v$, $e \nmid 2^s v$, $e = 2^i l'$, $l'|v, i = s+1$ and $f|2^{s+1}v$, $f = 2^k m'$, $2^k m'|2^{s+1}v$, $m'|v$, $k \le s+1$.
- Thus $k \le i$ which contradicts (*).

- The hypothesis implies that $\left(\frac{a}{p}\right)_L = 1$, $\left(\frac{a}{q}\right)_L = -1$.
- By Euler $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.
- Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$.
- Then $e \,\Big|\, \frac{p-1}{2} = 2^{j-1}l, f|q-1 = 2^k m, f \nmid \frac{q-1}{2}, j \le k$
- Thus $e = 2^i l'$, $f = 2^k m'$ with $0 \le i \le j-1$, $l'|l$, $m'|m$.
- In particular $0 \le i < j \le k$ (*).
- Recall that we are supposing that n divides exactly one of $a^v - 1, a^v + 1, \ldots, a^{2^{u-1}v} + 1$.
- If $n|a^v - 1$, then $a^v \equiv 1 \pmod{q}$ and $f|v$.
- But f is even and v is odd, so this is impossible.
- If $n|a^{2^s v} + 1$ for some s with $0 \le s \le u-1$, then $a^{2^{s+1}v} \equiv 1 \pmod{n}$, $a^{2^s v} \equiv -1 \pmod{n}$.
- Thus $e|2^{s+1}v$, $e \nmid 2^s v$, $e = 2^i l'$, $l'|v, i = s+1$ and $f|2^{s+1}v$, $f = 2^k m'$, $2^k m'|2^{s+1}v$, $m'|v$, $k \le s+1$.
- Thus $k \le i$ which contradicts (*).
- Hence a is a witness.

- Note that the previous theorem depends on the theory of quadratic residues and non-residues.

- Note that the previous theorem depends on the theory of quadratic residues and non-residues.
- Thus it should be no surprise that showing that there is a small witness is similar to showing that there are small quadratic non-residues.

- Note that the previous theorem depends on the theory of quadratic residues and non-residues.
- Thus it should be no surprise that showing that there is a small witness is similar to showing that there are small quadratic non-residues.
- Thus the best bound for a leads to questions which have a similar provenance to that concerning the least quadratic non-residue $n_2(p)$ discussed in Chapter 5.

- Note that the previous theorem depends on the theory of quadratic residues and non-residues.
- Thus it should be no surprise that showing that there is a small witness is similar to showing that there are small quadratic non-residues.
- Thus the best bound for a leads to questions which have a similar provenance to that concerning the least quadratic non-residue $n_2(p)$ discussed in Chapter 5.
- In particular Linnik's work quoted there suggests that any composite n with no small witnesses would be incredibly rare.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.
- 1. Check n for small factors not exceeding $\log n$.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.
- 1. Check n for small factors not exceeding $\log n$.
- 2. Check that n is not a prime power.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.
- 1. Check n for small factors not exceeding $\log n$.
- 2. Check that n is not a prime power.
- 3. Find u and v with $n-1=2^u v$ with v odd.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.
- 1. Check n for small factors not exceeding $\log n$.
- 2. Check that n is not a prime power.
- 3. Find u and v with $n-1=2^u v$ with v odd.
- 4. For each a with $2 \le a \le \min\left\{2(\log n)^2, n-2\right\}$ check the statements $n|a^v-1$, $n|a^v+1, \ldots, n|a^{2^{u-1}v}+1$. If easy to do restrict a to being prime.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.
- 1. Check n for small factors not exceeding $\log n$.
- 2. Check that n is not a prime power.
- 3. Find u and v with $n-1=2^u v$ with v odd.
- 4. For each a with $2 \le a \le \min\left\{2(\log n)^2, n-2\right\}$ check the statements $n|a^v-1$, $n|a^v+1, \ldots, n|a^{2^{u-1}v}+1$. If easy to do restrict a to being prime.
- 5. If there is an a such that they are all false, stop and declare that n is composite and a is a witness.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.
- 1. Check n for small factors not exceeding $\log n$.
- 2. Check that n is not a prime power.
- 3. Find u and v with $n-1=2^u v$ with v odd.
- 4. For each a with $2 \le a \le \min\left\{2(\log n)^2, n-2\right\}$ check the statements $n|a^v-1$, $n|a^v+1, \ldots, n|a^{2^{u-1}v}+1$. If easy to do restrict a to being prime.
- 5. If there is an a such that they are all false, stop and declare that n is composite and a is a witness.
- 6. If no witness a found with $a \le \min\left\{2(\log n)^2, n-2\right\}$, then declare that n is prime.

- No-one has come close to disproving the Riemann Hypothesis so I recommend the second approach, *via* following algorithm.
- Assume that n is odd.
- 1. Check n for small factors not exceeding $\log n$.
- 2. Check that n is not a prime power.
- 3. Find u and v with $n-1=2^u v$ with v odd.
- 4. For each a with $2 \le a \le \min\left\{2(\log n)^2, n-2\right\}$ check the statements $n|a^v-1$, $n|a^v+1, \ldots, n|a^{2^{u-1}v}+1$. If easy to do restrict a to being prime.
- 5. If there is an a such that they are all false, stop and declare that n is composite and a is a witness.
- 6. If no witness a found with $a \le \min\left\{2(\log n)^2, n-2\right\}$, then declare that n is prime.
- There are one further wrinkle that can be tried. Before doing the divisibility checks in 4, check that $(a,n)=1$ (or $a \nmid n$ if a is prime) because otherwise one has a proper divisor of n and not only is n composite but one has found a factor.

- A trivial but illustrative

Example 3

Let $n = 133$. Then

$$n - 1 = 2^2 \times 33$$

and

$$2^{33} \equiv 50 \pmod{133},\ 2^{66} \equiv 106 \pmod{133}$$

so

$$n \nmid 2^{33} - 1,\ n \nmid 2^{33} + 1,\ n \nmid 3^{66} + 1$$

Thus n is composite and a is a witness.

- Primality in a non-trivial case is best left to a computer program. But to illustrate the method here is an example.

Example 4

Let $n = 11$. Then $n - 1 = 2 \times 5$ and we have the following

$$\begin{aligned} 2^5 &= 32 \equiv -1 \pmod{11}, & 3^5 &= 243 \equiv 1 \pmod{11} \\ 4^5 &\equiv (2^5)^2 \equiv 1 \pmod{11}, & 5^5 &= 3125 \equiv 1 \pmod{11} \\ 6^5 &= (-5)^5 \equiv -1 \pmod{11}, & 7^5 &= (-4)^5 \equiv -1 \pmod{11} \\ 8^5 &= (-3)^5 \equiv -1 \pmod{11}, & 9^5 &= (3^5)^2 \equiv 1 \pmod{11} \end{aligned}$$

There is no witness, so n is prime. Of course we knew that!

- Primality in a non-trivial case is best left to a computer program. But to illustrate the method here is an example.

Example 4

Let $n = 11$. Then $n - 1 = 2 \times 5$ and we have the following

$$\begin{aligned} 2^5 &= 32 \equiv -1 \pmod{11}, & 3^5 &= 243 \equiv 1 \pmod{11} \\ 4^5 &\equiv (2^5)^2 \equiv 1 \pmod{11}, & 5^5 &= 3125 \equiv 1 \pmod{11} \\ 6^5 &= (-5)^5 \equiv -1 \pmod{11}, & 7^5 &= (-4)^5 \equiv -1 \pmod{11} \\ 8^5 &= (-3)^5 \equiv -1 \pmod{11}, & 9^5 &= (3^5)^2 \equiv 1 \pmod{11} \end{aligned}$$

There is no witness, so n is prime. Of course we knew that!

- Primality in a non-trivial case is best left to a computer program. But to illustrate the method here is an example.

Example 4

Let $n = 11$. Then $n - 1 = 2 \times 5$ and we have the following

$$\begin{aligned} 2^5 &= 32 \equiv -1 \pmod{11}, & 3^5 &= 243 \equiv 1 \pmod{11} \\ 4^5 &\equiv (2^5)^2 \equiv 1 \pmod{11}, & 5^5 &= 3125 \equiv 1 \pmod{11} \\ 6^5 &= (-5)^5 \equiv -1 \pmod{11}, & 7^5 &= (-4)^5 \equiv -1 \pmod{11} \\ 8^5 &= (-3)^5 \equiv -1 \pmod{11}, & 9^5 &= (3^5)^2 \equiv 1 \pmod{11} \end{aligned}$$

There is no witness, so n is prime. Of course we knew that!

- Even for a number like 211 this would be heavy handed and is one of the reasons for an initial range of trial division. For large n one will only need to consider a relatively small range of a.

- We have already used the term "probabilistic" informally in the previous section without saying precisely what we mean.

Definition 5

Suppose that we have a finite set $\mathcal{A}$ of cardinality M, and a subset $\mathcal{B}$ of cardinality N. In general we will suppose that the elements of $\mathcal{B}$ have some special property that marks them out from those in the complement of $\mathcal{B}$ with respect to $\mathcal{A}$. If we pick an element of $a \in \mathcal{A}$ without fear or favour, then we define the probability that $a \in \mathcal{B}$ as

$$\frac{N}{M}.$$

- We have already used the term "probabilistic" informally in the previous section without saying precisely what we mean.

Definition 5

Suppose that we have a finite set $\mathcal{A}$ of cardinality M, and a subset $\mathcal{B}$ of cardinality N. In general we will suppose that the elements of $\mathcal{B}$ have some special property that marks them out from those in the complement of $\mathcal{B}$ with respect to $\mathcal{A}$. If we pick an element of $a \in \mathcal{A}$ without fear or favour, then we define the probability that $a \in \mathcal{B}$ as

$$\frac{N}{M}.$$

- It is also possible to define probability for elements of infinite sets, but then we have to be concerned with how we measure the size of the sets, and this involves the much more sophisticated subject of measure theory.

- We have already used the term “probabilistic” informally in the previous section without saying precisely what we mean.

Definition 5

Suppose that we have a finite set $\mathcal{A}$ of cardinality M, and a subset $\mathcal{B}$ of cardinality N. In general we will suppose that the elements of $\mathcal{B}$ have some special property that marks them out from those in the complement of $\mathcal{B}$ with respect to $\mathcal{A}$. If we pick an element of $a \in \mathcal{A}$ without fear or favour, then we define the probability that $a \in \mathcal{B}$ as

$$\frac{N}{M}.$$

- It is also possible to define probability for elements of infinite sets, but then we have to be concerned with how we measure the size of the sets, and this involves the much more sophisticated subject of measure theory.
- Fortunately we have no need of that here.

- This comes up frequently

Example 6

Let $\mathcal{A} = \{1, 2, \ldots, M\}$, let $q \in \mathbb{N}$ and $0 \le r < q$ and let

$$\mathcal{B}(q, r) = \{a \in \mathcal{A} : a \equiv r \pmod q\}.$$

Then $$N = \operatorname{card} \mathcal{B}(q, r) = 1 + \left\lfloor \frac{M - r}{q} \right\rfloor.$$

Now $$\frac{M - r}{q} - 1 < \left\lfloor \frac{M - r}{q} \right\rfloor \le \frac{M - r}{q}$$

and so $$-1 < -\frac{r}{q} < N - \frac{M}{q} \le 1 - \frac{r}{q} < 1.$$

Therefore $$-\frac{1}{M} + \frac{1}{q} < \frac{N}{M} < \frac{1}{q} + \frac{1}{M}.$$

Thus if M is large compared with q, then we can see that the probability that an element of a is in $\mathcal{B}$ is close to $\frac{1}{q}$.

- Consider the following.

- Consider the following.
- Suppose we have a class of with s students.

- Consider the following.
- Suppose we have a class of with s students.
- What are the chances that there are two with the same birthday?

- Consider the following.
- Suppose we have a class of with s students.
- What are the chances that there are two with the same birthday?
- For simplicity assume there are no leap years.

- Consider the following.
- Suppose we have a class of with s students.
- What are the chances that there are two with the same birthday?
- For simplicity assume there are no leap years.
- Well in the population at large there are 365^2 pairs of birthdays and of those pairs only 365 will be the same.

- Consider the following.
- Suppose we have a class of with s students.
- What are the chances that there are two with the same birthday?
- For simplicity assume there are no leap years.
- Well in the population at large there are 365^2 pairs of birthdays and of those pairs only 365 will be the same.
- Thus if you pick a random pair of people you might conclude that only one in 365 pairs have the same birthday so the class will have to be really large, with getting on for at least 365 members.

- Consider the following.
- Suppose we have a class of with s students.
- What are the chances that there are two with the same birthday?
- For simplicity assume there are no leap years.
- Well in the population at large there are 365^2 pairs of birthdays and of those pairs only 365 will be the same.
- Thus if you pick a random pair of people you might conclude that only one in 365 pairs have the same birthday so the class will have to be really large, with getting on for at least 365 members.
- The fallacy here is that we are dealing with more than just pairs.

- Look at it this way.

- Look at it this way.
- Suppose we have a group of s people.

- Look at it this way.
- Suppose we have a group of s people.
- The number of possible configurations of birthdays for s people is 365^s - each person can have any one of 365 possibilities.

- Look at it this way.
- Suppose we have a group of s people.
- The number of possible configurations of birthdays for s people is 365^s - each person can have any one of 365 possibilities.
- Let $\mathcal{A}$ be the set of all such configurations.

- Look at it this way.
- Suppose we have a group of s people.
- The number of possible configurations of birthdays for s people is 365^s - each person can have any one of 365 possibilities.
- Let $\mathcal{A}$ be the set of all such configurations.
- One can think of the elements as being s-tuples $(d_1, d_2, \ldots, d_s)$ with each entry in the s-tuple being a number d_j in the range $\{1, 2, \ldots, 365\}$.

- Look at it this way.
- Suppose we have a group of s people.
- The number of possible configurations of birthdays for s people is 365^s - each person can have any one of 365 possibilities.
- Let $\mathcal{A}$ be the set of all such configurations.
- One can think of the elements as being s-tuples $(d_1, d_2, \ldots, d_s)$ with each entry in the s-tuple being a number d_j in the range $\{1, 2, \ldots, 365\}$.
- Then $M = \operatorname{card} \mathcal{A} = 365^s$

- In how many of those s-tuples could all the entries (birthdays) be different?

- In how many of those s-tuples could all the entries (birthdays) be different?
- Let $\mathcal{B}$ be that subset of $\mathcal{A}$ and let $N = \operatorname{card}\mathcal{B}$. Then

$$N = 365(365-1)\dots(365-s+1) \qquad (2.3)$$

- In how many of those s-tuples could all the entries (birthdays) be different?
- Let $\mathcal{B}$ be that subset of $\mathcal{A}$ and let $N = \operatorname{card} \mathcal{B}$. Then

$$N = 365(365-1)\dots(365-s+1) \tag{2.3}$$

- See it this way. The first person, d_1, has 365 choices.

- In how many of those s-tuples could all the entries (birthdays) be different?
- Let $\mathcal{B}$ be that subset of $\mathcal{A}$ and let $N = \operatorname{card}\mathcal{B}$. Then

$$N = 365(365-1)\dots(365-s+1) \tag{2.3}$$

- See it this way. The first person, d_1, has 365 choices.
- Then the second d_2 only has 364 choices for d_2, and so on.

- In how many of those s-tuples could all the entries (birthdays) be different?
- Let $\mathcal{B}$ be that subset of $\mathcal{A}$ and let $N = \operatorname{card}\mathcal{B}$. Then

$$N = 365(365-1)\dots(365-s+1) \tag{2.3}$$

- See it this way. The first person, d_1, has 365 choices.
- Then the second d_2 only has 364 choices for d_2, and so on.
- Thus the number of ways in which all the birthdays are different is the number of s-tuples in which the entries are different and this is (2.3).

- In how many of those s-tuples could all the entries (birthdays) be different?
- Let $\mathcal{B}$ be that subset of $\mathcal{A}$ and let $N = \operatorname{card} \mathcal{B}$. Then

$$N = 365(365-1)\dots(365-s+1) \tag{2.3}$$

- See it this way. The first person, d_1, has 365 choices.
- Then the second d_2 only has 364 choices for d_2, and so on.
- Thus the number of ways in which all the birthdays are different is the number of s-tuples in which the entries are different and this is (2.3).
- Thus the probability that a member of $\mathcal{A}$ is in $\mathcal{B}$ is

$$\rho(s) = \frac{N}{M} = \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\dots\left(1 - \frac{s-1}{365}\right).$$

- In how many of those s-tuples could all the entries (birthdays) be different?
- Let $\mathcal{B}$ be that subset of $\mathcal{A}$ and let $N = \operatorname{card} \mathcal{B}$. Then

$$N = 365(365-1)\dots(365-s+1) \tag{2.3}$$

- See it this way. The first person, d_1, has 365 choices.
- Then the second d_2 only has 364 choices for d_2, and so on.
- Thus the number of ways in which all the birthdays are different is the number of s-tuples in which the entries are different and this is (2.3).
- Thus the probability that a member of $\mathcal{A}$ is in $\mathcal{B}$ is

$$\rho(s) = \frac{N}{M} = \left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\dots\left(1-\frac{s-1}{365}\right).$$

- Thus the probability that at least two members of the class share a birthday is

$$1-\rho(s) = 1-\left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\dots\left(1-\frac{s-1}{365}\right).$$

s	$\rho(s)$	s	$\rho(s)$
21	$.5563\dots$	22	$.5243\dots$
23	$.4927\dots$	24	$.4616\dots$
25	$.4313\dots$	26	$.4017\dots$
27	$.3731\dots$	28	$.3455\dots$
29	$.3190\dots$	30	$.2936\dots$
31	$.2695\dots$	32	$.2466\dots$
33	$.2250\dots$	34	$.2046\dots$
35	$.1856\dots$	36	$.1678\dots$
37	$.1512\dots$	38	$.1359\dots$
39	$.1217\dots$	40	$.1087\dots$
41	$.0968\dots$	42	$.0859\dots$
43	$.0760\dots$	44	$.0671\dots$
45	$.0590\dots$	46	$.0517\dots$
47	$.0452\dots$	48	$.0394\dots$
49	$.0342\dots$	50	$.0296\dots$

The probability $\rho(s)$ that a class of size s has no two birthdays the same.

- Thus if the class has 23 members, then it is more likely than not that there will be two people sharing a birthday.

- Thus if the class has 23 members, then it is more likely than not that there will be two people sharing a birthday.
- This class has 48 members so it is practically certain that two members will have the same birthday.

- Thus if the class has 23 members, then it is more likely than not that there will be two people sharing a birthday.
- This class has 48 members so it is practically certain that two members will have the same birthday.
- This is the *birthday paradox* and its generalization plays an important rôle in establishing coincidences in computations.

- Thus if the class has 23 members, then it is more likely than not that there will be two people sharing a birthday.
- This class has 48 members so it is practically certain that two members will have the same birthday.
- This is the *birthday paradox* and its generalization plays an important rôle in establishing coincidences in computations.
- We need to generalize this.

- Thus if the class has 23 members, then it is more likely than not that there will be two people sharing a birthday.
- This class has 48 members so it is practically certain that two members will have the same birthday.
- This is the *birthday paradox* and its generalization plays an important rôle in establishing coincidences in computations.
- We need to generalize this.
- Let D be the number of possible values for each entry in the s-tuple - so we are now supposing that our year has D days!

- Thus if the class has 23 members, then it is more likely than not that there will be two people sharing a birthday.
- This class has 48 members so it is practically certain that two members will have the same birthday.
- This is the *birthday paradox* and its generalization plays an important rôle in establishing coincidences in computations.
- We need to generalize this.
- Let D be the number of possible values for each entry in the s-tuple - so we are now supposing that our year has D days!
- Then $M = \text{card}\, A = D^s$ and $N = \text{card}\, B$ is

$$N = D(D-1)\dots(D-N+1)$$

so that the probability that there are no coincidences in the entries in an arbitrary s-tuple is

$$\frac{N}{M} = \left(1 - \frac{1}{D}\right)\left(1 - \frac{2}{D}\right)\dots\left(1 - \frac{s-1}{D}\right).$$

- $$\rho(s) = \frac{N}{M} = \left(1 - \frac{1}{D}\right)\left(1 - \frac{2}{D}\right)\dots\left(1 - \frac{s-1}{D}\right).$$

- $$\rho(s) = \frac{N}{M} = \left(1 - \frac{1}{D}\right)\left(1 - \frac{2}{D}\right)\dots\left(1 - \frac{s-1}{D}\right).$$
- Thus if this number is smaller than 0.5 we could conclude that amongst all the s-tuples it is more likely that at least one s-tuple will have two entries the same than that all s-tuples will have all entries different.

- $$\rho(s) = \frac{N}{M} = \left(1 - \frac{1}{D}\right)\left(1 - \frac{2}{D}\right)\dots\left(1 - \frac{s-1}{D}\right).$$
- Thus if this number is smaller than 0.5 we could conclude that amongst all the s-tuples it is more likely that at least one s-tuple will have two entries the same than that all s-tuples will have all entries different.
- In a particular case we might ask how large s has to be in terms of D that this probability is smaller than some number σ where $0 < \sigma < 1$,

- $$\rho(s) = \frac{N}{M} = \left(1 - \frac{1}{D}\right)\left(1 - \frac{2}{D}\right)\dots\left(1 - \frac{s-1}{D}\right).$$
- Thus if this number is smaller than 0.5 we could conclude that amongst all the s-tuples it is more likely that at least one s-tuple will have two entries the same than that all s-tuples will have all entries different.
- In a particular case we might ask how large s has to be in terms of D that this probability is smaller than some number σ where $0 < \sigma < 1$,
- so that
$$\rho(s) = \prod_{k=1}^{s-1}\left(1 - \frac{k}{D}\right) < \sigma.$$

- $$\rho(s) = \frac{N}{M} = \left(1 - \frac{1}{D}\right)\left(1 - \frac{2}{D}\right)\dots\left(1 - \frac{s-1}{D}\right).$$
- Thus if this number is smaller than 0.5 we could conclude that amongst all the s-tuples it is more likely that at least one s-tuple will have two entries the same than that all s-tuples will have all entries different.
- In a particular case we might ask how large s has to be in terms of D that this probability is smaller than some number σ where $0 < \sigma < 1$,
- so that
$$\rho(s) = \prod_{k=1}^{s-1}\left(1 - \frac{k}{D}\right) < \sigma.$$
- Since it is easier to work with sums than products, we can rewrite this as
$$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1}\log\frac{1}{1-\frac{k}{D}} > \log\frac{1}{\sigma}.$$

- $$\log \frac{1}{\rho(s)} = \sum_{k=1}^{s-1} \log \frac{1}{1 - \frac{k}{D}}.$$

- $$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1} \log\frac{1}{1-\frac{k}{D}}.$$
- It makes sense to assume $s \le D$, and so by the expansion for the logarithmic factor,

$$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1}\sum_{h=1}^{\infty}\frac{k^h}{hD^h}.$$

- $$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1}\log\frac{1}{1-\frac{k}{D}}.$$
- It makes sense to assume $s \le D$, and so by the expansion for the logarithmic factor,

$$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1}\sum_{h=1}^{\infty}\frac{k^h}{hD^h}.$$

- and since all the terms are positive we have

$$\log\frac{1}{\rho(s)} > \sum_{k=1}^{s-1}\frac{k}{D} = \frac{s(s-1)}{2D},$$

- $$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1}\log\frac{1}{1-\frac{k}{D}}.$$
- It makes sense to assume $s \le D$, and so by the expansion for the logarithmic factor,
$$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1}\sum_{h=1}^{\infty}\frac{k^h}{hD^h}.$$
- and since all the terms are positive we have
$$\log\frac{1}{\rho(s)} > \sum_{k=1}^{s-1}\frac{k}{D} = \frac{s(s-1)}{2D},$$
- Thus
$$\rho(s) < \exp\left(-\frac{s(s-1)}{2D}\right).$$

- If

$$\exp\left(-\frac{s(s-1)}{2D}\right) < \sigma,$$

then

$$\rho(s) < \exp\left(-\frac{s(s-1)}{2D}\right) < \sigma.$$

- If
$$\exp\left(-\frac{s(s-1)}{2D}\right) < \sigma,$$
then
$$\rho(s) < \exp\left(-\frac{s(s-1)}{2D}\right) < \sigma.$$
- Thus we see that, once s gets somewhat larger than $\sqrt{D}$, when we pick an s-tuple at random we are quite likely to find two entries the same.

- If
$$\exp\left(-\frac{s(s-1)}{2D}\right) < \sigma,$$
then
$$\rho(s) < \exp\left(-\frac{s(s-1)}{2D}\right) < \sigma.$$
- Thus we see that, once s gets somewhat larger than $\sqrt{D}$, when we pick an s-tuple at random we are quite likely to find two entries the same.
- Even for a number as small as $D = 365$ this quite crude approximation shows that $\rho(s) < \frac{1}{2}$ when $s = 23$.

- If
$$\exp\left(-\frac{s(s-1)}{2D}\right) < \sigma,$$
then
$$\rho(s) < \exp\left(-\frac{s(s-1)}{2D}\right) < \sigma.$$
- Thus we see that, once s gets somewhat larger than $\sqrt{D}$, when we pick an s-tuple at random we are quite likely to find two entries the same.
- Even for a number as small as $D = 365$ this quite crude approximation shows that $\rho(s) < \frac{1}{2}$ when $s = 23$.
- Thus even if σ is taken to be quite small one does not have to take s much bigger than $\sqrt{D}$ to achieve the desired result.

- If
$$\exp\left(-\frac{s(s-1)}{2D}\right) < \sigma,$$
then
$$\rho(s) < \exp\left(-\frac{s(s-1)}{2D}\right) < \sigma.$$
- Thus we see that, once s gets somewhat larger than $\sqrt{D}$, when we pick an s-tuple at random we are quite likely to find two entries the same.
- Even for a number as small as $D = 365$ this quite crude approximation shows that $\rho(s) < \frac{1}{2}$ when $s = 23$.
- Thus even if σ is taken to be quite small one does not have to take s much bigger than $\sqrt{D}$ to achieve the desired result.
- In other words, if s is large compared with $\sqrt{D}$, then it will be almost certain that there will be coincidences.

- If
$$\exp\left(-\frac{s(s-1)}{2D}\right) < \sigma,$$
then
$$\rho(s) < \exp\left(-\frac{s(s-1)}{2D}\right) < \sigma.$$
- Thus we see that, once s gets somewhat larger than $\sqrt{D}$, when we pick an s-tuple at random we are quite likely to find two entries the same.
- Even for a number as small as $D = 365$ this quite crude approximation shows that $\rho(s) < \frac{1}{2}$ when $s = 23$.
- Thus even if σ is taken to be quite small one does not have to take s much bigger than $\sqrt{D}$ to achieve the desired result.
- In other words, if s is large compared with $\sqrt{D}$, then it will be almost certain that there will be coincidences.
- By the way, some attacks on security systems take advantage of this and we will make use of it later in one of the factoring attacks.