Repetition:

Euler φ-function $\varphi(n) = |\mathbb{Z}_n^*|$

$$a^{\varphi(n)} \equiv 1 \pmod n$$ Euler

Special case for prime p: Fermat

6.1 Probabilistic Primality testing

FPT - Fermat Primality Test

- Select randomly some $a \in \{2, \dots, n-1\}$. Compute $a^{n-1} \bmod n$
- $a^{n-1} \not\equiv 1 \pmod n \Rightarrow$ "n composite"
- Otherwise declare "n prime"

It holds that

$$n \text{ composite}, \; a \in \mathbb{Z}_n \setminus \mathbb{Z}_n^* \Rightarrow a^{n-1} \not\equiv 1 \pmod n$$

Proof. Suppose $a^{n-1} \equiv 1 \pmod n \Rightarrow a^{-1}$ exists, namely $a^{-1} = a^{n-2}$

$\Rightarrow \gcd(a, n) = 1 \Rightarrow a \in \mathbb{Z}_n^*$. Contradiction

The least favourable case for the FPT is

$$n \text{ composite and } a^{n-1} \equiv 1 \pmod n \quad \forall a \in \mathbb{Z}_n^*$$

Such numbers are called Carmichael numbers. The first ones are

561, 1105, 1729, 2465, 2821, 6601, 29341, 172081, ...

Prop. 6.3 Let n be composite and odd, no Carmichael number

Then $|\{a \in \mathbb{Z}_n \setminus \{0\} \mid a^{n-1} \not\equiv 1 \pmod n\}| \geq \frac{n}{2}$

Proof: Script

Hence, for alg. FPT, provided n is not a Carmichael number

$P(\text{FPT states "}n\text{ composite"} \mid \text{"}n\text{ composite"}) \geq \frac{1}{2}$, or equivalently

$P(\text{FPT states "}n\text{ prime"} \mid \text{"}n\text{ composite"}) \leq \frac{1}{2}$ Moreover

$P(\text{FPT states "}n\text{ prime"} \mid \text{"}n\text{ prime"}) = 1$

Advantages: Very simple, easy to implement, fast,
error probability is less than $\frac{1}{2^m}$ after m independent trials.

In the following: Probabilistic primality test satisfying for any $n \in \mathbb{N}$

1. n prime $\Rightarrow$ Alg declares "n prime" with prob. 1
2. n composite $\Rightarrow$ " " "n composite" with prob. $\geq 3/4$

Def 6.4 Let $n = 1 + q \cdot 2^k$, q odd $k \in \mathbb{N}_0$ (each odd integer has a representation like this)

Let $a \in \mathbb{N}$, $2 \leq a \leq n-1$

· a is called a strong witness (to compositeness), if

$$(i) \quad a^q \not\equiv 1 \pmod n$$

$$(ii) \quad a^{q \cdot 2^i} \not\equiv -1 \pmod n \quad \forall\, i = 0, \dots, k-1$$

$$(\not\equiv n-1)$$

Abbr. $a \in W(n)$

Prop 6.5 $\exists\, a \in W(n) \Rightarrow n$ is composite

Proof: Suppose $a \in W(n)$ and n is prime. By Fermat's theorem

$$a^{n-1} = a^{q \cdot 2^k} \equiv 1 \pmod n$$

Consider successive squares

$$\underbrace{a^q}_{\not\equiv 1 \pmod n}, a^{q \cdot 2}, a^{q \cdot 2^2}, \dots\dots, \underbrace{a^{q \cdot 2^k}}_{\equiv 1 \pmod n}$$

Let $j = \max\{0 \leq i \leq k-1 \mid a^{q \cdot 2^i} \not\equiv 1 \pmod n, a^{q \cdot 2^{i+1}} \equiv 1 \pmod n\}$

$b = a^{q \cdot 2^j}$, s.t. $b \not\equiv 1 \pmod n$ and $b^2 \equiv 1 \pmod n$

n prime $\Rightarrow \mathbb{Z}_n$ is a field $\Rightarrow b \equiv 1$ or $b \equiv -1 \pmod n$

In summary $b \equiv (-1) \pmod n$ Contradiction to (ii)

There are only a few $a \in \{2, \dots, n-1\}$ with $a \notin W(n)$. More precisely

Theorem 6.6 (Rabin, 1980)

For any odd, composite $n \in \mathbb{N}$ it holds that

$$\left| \{ a \mid 2 \le a \le n-1 , a \notin W(n) \} \right| \le \frac{n}{4}$$

Proof: • Rabin, 1980, Probabilistic alg. for testing primality J. Number Theory, 12, 128-138

• Koblitz, A course in Number Theory and Cryptography Springer, New York, 1994, p130ff

Hence, choosing a at random in $\{2, \dots, n-1\}$ with $a \notin W(n)$ has probability $\le \frac{1}{4}$

MRPT - Miller-Rabin-Primality-Test

- Determine $n = 1 + q \cdot 2^k$, q odd, $k \in \mathbb{N}_0$
- Choose $a \in \{2, \dots, n-1\}$ at random
- $y = a^q \bmod n$
- if $y = 1$ then
  return "n is prime" // $a \notin W(n)$
  end if
- for i from 1 to k
  if $y = n-1$ then // $a \notin W(n)$
  return "n is prime"
  end if
  $y \Leftarrow y^2 \bmod n$
  end for
- return "n composite" $a \in W(n)$

Application: Repeat MRPT M times with independently selected $a \in \{2, \dots, n-1\}$

If MRPT returns M times "n prime", decide "n prime"
otherwise decide "n is composite"

$$P(\text{decide "}n\text{ prime"} \mid \text{"}n\text{ composite"}) \leq \left(\frac{1}{4}\right)^M$$

$$P(\text{decide "}n\text{ prime"} \mid \text{"}n\text{ prime"}) = 1$$

Exponentially decreasing bound: $\frac{1}{4^{10}} \approx 0.95 \cdot 10^{-6}$, $\frac{1}{4^{20}} \approx 0.91 \cdot 10^{-12}$

Remarks:

Since Aug. 2002 there is a polynomial time deterministic alg that determines whether an input number n is prime or composite.

M. Agrawal, N. Kayal, N. Saxena: PRIMES is in P
Annals of Mathematics, 160 (2004), 781–793

General assessment of this work

- There is a polynomial time alg. to prove that a number is prime or composite
- Much slower than the probabilistic alg. MRPT, most times inacceptably slow
- Feeling: We can live with some error probability of 2^{-1000}, say.

How to find large prime numbers:

Choose odd $n \in \mathbb{N}$ (n large). Iterate $n \leftarrow n+2$ until a prime number n is found by MRPT

The prime number theorem states:

Theorem 6.7 It holds

$$|\{p \mid p \leq n,\ p \text{ prime}\}| \sim \frac{n}{\ln(n)}$$

Hence, the prob. that a randomly chosen $m \leq n \in \mathbb{N}$ is prime is $\sim \frac{1}{\ln(n)}$

Ex. $n = 2^{512}$, select only odd integers $\frac{2}{\ln(2^{512})} \approx \frac{1}{177.4} \approx 5.64 \cdot 10^{-3}$

6.2 The Integer Factorization Problem

"Easy": Decide whether a given integer n is composite

"Hard": Find its prime factorization

Pollards $p-1$ factoring alg.

Given composite n. Assume that n has a prime factor p such that $p-1$ has all prime factors $\leq B$.

Let C s.t. $p-1 \mid C$, e.g. $C = B!$ has this property (only) with high probability

Algorithm Pollard-$(p-1)$

- Choose $a > 1$ (often $a = 2$)
- Compute $b = a^C \bmod n$
- Compute $d = \gcd(b-1, n)$
- If $1 < d < n$, then d is a non-trivial factor of n

Proof that Pollard-$(p-1)$ is correct:

Assume p is a prime factor of n s.t. $p-1$ has all prime factors $\leq B$.

Let $p-1 \mid C$, e.g. $C = B!$, i.e., $C = k(p-1)$ for some $k \in \mathbb{N}$

By Fermat's little theorem

$$a^C \equiv \left(a^{p-1}\right)^k \equiv 1 \pmod p$$

Hence, $a^C - 1 \equiv 0 \pmod p$ such that

$p \leq \gcd(b-1, n)$ is a factor of n

Remarks: a) If choosing $c = B!$ then compute $a^{B!} \bmod n$ as follows

$$b_0 = a \qquad b_j = b_{j-1}^{j} \bmod n \qquad j = 1, \dots, B$$

b) To overcome the possibility that $p-1 \nmid B!$ substitute $B!$ by

$$c = \prod_{\substack{q \le B \\ q \text{ prime}}} q^{\lfloor \frac{\ln(n)}{\ln(q)} \rfloor} \qquad \text{It holds} \quad q^{\lfloor \frac{\ln(n)}{\ln(q)} \rfloor} \le q^{\log_q(n)} = n$$

$$q^{\lceil \frac{\ln(n)}{\ln(q)} \rceil} \ge q^{\log_q(n)} = n$$

Moreover $c << B$

c) You might be unlucky that $\gcd(b-1, n) = n$

($\Leftrightarrow$ q has also some small prime factors, where $n = p \cdot q$)

To protect against Pollard-$(p-1)$ select

$n = p \cdot q$ s.t $p-1$ and $q-1$ have at least one large prime ~~number~~ factor. How?

e.g. Sophie-Germain's primes $p = 2 \cdot r + 1$ p, r are prime

(or replace 2 by some integer k)