Lecture 02

Jose Capco (jcapco@risc.jku.at)

Notice that the Fermat's little theorem is the statement that for any prime $p \in \mathbb{P}$ and any $a \in \mathbb{F}_p \backslash \{0\}$ one has

$$a^{p-1} = 1 \bmod p$$

The question is whether requiring $a^{n-1} = 1 \bmod n$, for all $a \in \mathbb{N}$ such that $(a, n) = 1$, implies that n is a prime number. If for such an n an a satisfy this then we say that n *is a (Fermat) pseudoprime base* a. Even if n is a pseudoprime base any a coprime to n, n may still not be a prime number. This led to the study of Carmichael numbers

Definition. A number $n \in 2\mathbb{N} + 1$ is called *Carmichael* iff it is composite and for all $a = \{1, \ldots, n-1\}$ coprime to n one has

$$a^{n-1} = 1 \bmod n$$

Korselt seems to first come with the idea of Carmichael number, but Carmichaal probably was the first to show their existence. Here we give a characterization of Carmichael numbers due to Korselt and the key idea in the proof is Chinese Remainder Theorem and primitive roots ...

Korselt Criterion. A number $n \in 2\mathbb{N} + 1$ is Carmichael iff the following holds

- n is square-free
- If $p \in \mathbb{P}$ such that $p \mid n$ then $(p-1) \mid (n-1)$

Proof. "$\Leftarrow$" Write $n = p_1 p_2 \cdots p_k$ where p_i are the distinct primes dividing n. Let $a \in \{1, \ldots, n-1\}$ be coprime with n then, by the Chinese Remainder Theorem, we can identify $a \in (\mathbb{Z}/n\mathbb{Z})^*$ with $(a_1, a_2, \ldots, a_k) \in \prod_{i=1}^{k} (\mathbb{Z}/p_i\mathbb{Z})^*$. So we can identify $a^{n-1} \in (\mathbb{Z}/n)^*$ with

$$(a_1^{n-1}, \ldots, a_k^{n-1}) \in \prod_{i=1}^{k} (\mathbb{Z}/p_i\mathbb{Z})^*$$

But $p_i - 1 \mid n - 1$ for all $i = 1, \ldots, k$ thus

$$a_i^{n-1} = a_i^{p_i - 1} = 1 \bmod p_i \qquad \forall i = 1, \ldots, k$$

and so $a^{n-1} = 1 \bmod n$.

"$\Rightarrow$" We prove the first part by contradiction. Let $p \in \mathbb{P}$ and $p^2 \mid n$. Write $n = p^k m$, where m and p are coprime (so $k \geq 2$). By the Chinese Remainder Theorem there is an $a \in \mathbb{N}$ such that $a = 1 + p \bmod p^k$ and $a = 1 \bmod m$ (observe that $(a, n) = 1$). Because a is Carmichael, $a^{n-1} = 1 \bmod n$ so we apply the binomial expansion to get

$$1 = (1+p)^{n-1} = 1 + (n-1)p = 1 - p \bmod p^2$$

and this is a contradiction!

Now let $p \mid n$ then we know from the first part that $(p, n/p) = 1$ and so by the Chinese Remainder Theorem we can choose an $a \in \mathbb{N}$ such that a is a primitive root modulo p and $a \bmod n/p = 1$. We then see that $a^{n-1} = 1 \bmod p$ and so the order of $a \bmod p$, which is $p - 1$, must divide $n - 1$. □

Surprisingly, for the next 90 years after their introduction, we did not know (although it was long conjectured) whether there are infinite Carmichael numbers. In 1994, Alford,Pomerance and Granville showed that this is indeed the case. However, there are still lots of open problems on Carmichael numbers. One interesting example for a Carmichael number is the Ramanujan number 1729. It is the first Carmichael number of specific form (see the following exercise)

Example 1. The number 561 is the first Carmichael number. The Ramanujan number 1729 is the third Carmichael number.

Exercise 1.

1. Show that a Carmichael number must have at least three prime factors.
2. Show that if there are three primes of the form $6m+1$,$12m+1$ and $18m+1$ for some $m \in \mathbb{N}$ then their product is a Carmichael number. In your opinion (with justification), how many such Carmichael numbers would exist?
3. Let $C(x)$ is the number of Carmichael numbers less or equal $x \in \mathbb{R}^+$. Plot $C(x)$ over the positive real line and verify (however you can) that for sufficiently large x, we have $C(x) > x^{2/7}$ (if this is proven, then one proves the infinitude of Carmichael numbers).

We introduced Carmichael numbers because this motivates some prime proving algorithms due to Miller, Selfridge and Rabin (all from rather independent people).

Proposition 2. Let $n \in 2\mathbb{N}+1$ and suppose that $n-1 = 2 \bmod 4$ (i.e. $(n-1)/2$ is odd) then $a^{(n-1)/2} = \pm 1 \bmod n$ for all a such that $(a,n) = 1$ iff n is a prime number.

Proof. One direction is clear. Suppose, by contradiction, that n is composite. Then n should be Carmichael and by the Chinese Remainder Theorem we have a canonical isomorphism of groups

$$(\mathbb{Z}/n)^* \longrightarrow \prod_{i=1}^{k} (\mathbb{Z}/p_i)^*$$

for distinct odd primes $p_1, p_2, \ldots, p_k$ dividing n. We can thus choose an $a \in \mathbb{N}$ such that a is a primitive root mod p_1 and $a = 1 \bmod p_i$ for all $i = 2, \ldots, k$. Now, since n is Carmichael $p_1 - 1$ divides $n-1$ and since $\frac{n-1}{2}$ is odd, $\frac{p_1-1}{2}$ should be odd. Thus

$$a^{(n-1)/2} = a^{(p_1-1)/2} = -1 \bmod p_1$$

and so by the group isomorphism $a \bmod n \in (\mathbb{Z}/n)^*$ corresponds to $(-1, 1, \ldots, 1) \in \prod(\mathbb{Z}/p_i)^*$ but this does not correspond to $\pm 1 \in \mathbb{Z}/n$. □

Here is an Lemma for primitive roots of powers of prime:

Lemma 3. Let X be an indeterminate, p be an odd prime and $m \in \mathbb{N}$ such that $p \nmid m$ and suppose $e \in \mathbb{N}$, then the number of solutions for $X^m = 1 \bmod p^e$ in the ring $\mathbb{Z}/p^e$ is given by

$$\gcd(m, \phi(p^e)) = \gcd(m, p^{e-1}(p-1))$$

Example 4.

- The Lemma should also hold if $p = 2$ and m is odd. Let $p = 2, m = e = 3$ and let us count the number of solutions of $X^3 = 1 \bmod 2^3$. We can write elements in $\mathbb{Z}/8$ as

  $$\{0, 1, 2, 3, 4, -3, -2, -1\} \bmod 8$$

  We remove all the numbers that are not coprime with 2 and we note that $1 \bmod 8$ is the only solution to the above equation, since

  $$3^3 = 9 * 3 = 3 \bmod 8$$
  $$(-3)^3 = -3 \bmod 8$$
  $$(-1)^3 = -1 \bmod 8$$

  We also have $\gcd(m, p-1) = \gcd(3, 1) = 1$. If $p = 2$ we will always have 1 solution to an odd-root-of-unity module 2^e for any $e \in \mathbb{N}$

- Let $p = 3, m = 4, e = 2$. We want to solve for the solutions of $X^4 = 1 \bmod 3^2$. We write the elements of $\mathbb{Z}/9$ as follows

$$\{0, 1, 2, 3, 4, -4, -3, -2, -1\} \bmod 9$$

We look at all numbers above that are coprime to 3 and notice that we can use symmetric (i.e. $X^4 = (-X)^4 \bmod 9$). So 1 and -1 are clearly a solution and the other numbers yield

$$2^4 = (-2)^4 = 16 = 7 = -2 \bmod 9$$
$$4^4 = (-4)^4 = (-2)^2 = 4 \bmod 9$$

So there are indeed $\gcd(4, 3-1) = 2$ solutions.

Exercise 2. Give the proof of the above Lemma and find a general statement giving the number of roots of unity modulo a composite number.

The Miller-Rabin Test. Let $n \in 2\mathbb{N} + 9$ and suppose that $n - 1 = 2^t q$ for some $t \in \mathbb{N}$ and $q \in 2\mathbb{N} + 1$. Then n is prime iff for all $a \in \mathbb{N}$ relatively prime to n either of the following holds

$$\begin{aligned} &a^q = \pm 1 \bmod n \quad \text{or} \\ &a^{2^s q} = -1 \bmod n \quad \text{for some } s = 1, \ldots, t-1 \end{aligned} \tag{*}$$

Furthermore, only at most $1/4$ of the $a \bmod n \in (\mathbb{Z}/n)^*$ will satisfy (*) if n is not a prime.

If a satisfies (*) above then we say that n is a *strong psuedoprime* base a. Now we cannot go through all of the $a = 1, \ldots, n-1$ (esp. if n is really large). However by the above theorem we know that we will only get false positive (i.e. algorithm returns probable prime when n is not prime) using the above test only for at most 25% of the coprime element of n. So if we repeat this procedure k times for a particular n, the probability of a false positive is $\left(\frac{1}{4}\right)^k$.

This yields a probabilistic algorithm and is the most widely used algorithm for primality testing. Even if one uses a deterministic algorithm, the algorithm would take longer, so sometimes they use Miller-Rabin to check for primality before proceeding with the deterministic algorithm (because if Miller-Rabin tests results into a composite number then it is indeed one).

Exercise 3. For many of us, working with primes less than or equal to 10^{12} is sufficient. If we need to only check for primes less than 10^{12} (which are all known) and still not want to have a database of them, it is known that you only need to check with Miller-Rabin algorithm for all the coprime elements to n that are in the set

$$\{2, 3, 5, 7, 11\}$$

This set increases as you increase your upper bound. There are active research on the structure and size of these sets. Write a program that finds the least set of bases needed to check if a number $n \leq 100$ is a prime number using the Miller-Rabin test.

Proof. Proof of Miller-Rabin Test Suppose that n is an odd composite greater than 9 and has the factorization

$$n = \prod_{i=1}^{k} p_i^{e_i} \qquad p_i \in \mathbb{P}, e_i \in \mathbb{N}$$

and define $m \in \mathbb{N}$ be the maximum number such that $2^m \mid p_i - 1$ for all $i = 1, \ldots, k$ i.e.

$$m := \max\{l \,:\, 2^l \mid p_i - 1 \quad \forall i = 1, \ldots, k\}$$

and define $A(n) := \{a \bmod n \,:\, a^{2^{m-1} q} = \pm 1 \bmod n\}$.

The proof of this theorem is now divided into several steps ...

Step 1: Here we show that

$$A(n) \supset \{a \bmod n \,:\, a \text{ satisfies (*)}\}$$

Let a satisfy (*). If it satisfies $a^q = \pm 1 \bmod n$ then the result is clear. So we assume there is an $s = 1, \ldots t-1$ such that $a^{2^s q} = -1 \bmod n$. By the Chinese Remainder Theorem we then know that $a^{2^s q} = -1 \bmod p^e$ for all $p \in \mathbb{P}$ with $e \in \mathbb{N}$ such that $p^e \,||\, n$. This implies that $a^{2^s q} = -1 \bmod p$ for all $p \in \mathbb{P}$ such that $p \mid n$. Thus, $\mathrm{ord}_p(a) \mid 2^{s+1} q$ but $\mathrm{ord}_p(a) \nmid 2^s q$, in other words $2^{s+1} \,||\, \mathrm{ord}_p(a)$ for all $p \in \mathbb{P}$ with $p \mid n$. Because $\mathrm{ord}_p(a) \mid p-1$, one has $2^{s+1} \mid p-1$ for all such p. In other words $s+1 \leq m$. So $a^{2^{m-1} q} = 1 \bmod n$ if $m > s+1$ and $a^{2^{m-1} q} = -1 \bmod n$ if $m = s+1$.

The proof is complete if we can show that $\#A(n) < \phi(n)$. In other words we will show that

$$\frac{\#A(n)}{\#(\mathbb{Z}/n)^*} = \frac{\#A(n)}{\phi(n)} \leq \frac{1}{4}$$

To do this we will count $A(n)$ (the next step) in our next lecture session ... □