Complexity and Cryptography

Thomas Zeugmann

Hokkaido University
Laboratory for Algorithmics

https://www-alg.ist.hokudai.ac.jp/~thomas/COCR/

Lecture 4: Number Theoretic Algorithms

Linear Congruences I

In order to develop some more familiarity with calculations in the ring $\mathbb{Z}_m$ we continue by studying the solvability of the easiest form of congruences involving a variable, i.e., of linear congruences

$$ax \equiv c \mod b\ .$$

Linear Congruences I

In order to develop some more familiarity with calculations in the ring $\mathbb{Z}_m$ we continue by studying the solvability of the easiest form of congruences involving a variable, i.e., of linear congruences

$$ax \equiv c \mod b \, .$$

This is an important practical problem. There may be zero, one, or more than one solution satisfying $ax \equiv c \mod b$. The following theorem precisely characterizes the solvability of linear congruences:

Linear Congruences II

Theorem 1

Let $a, c \in \mathbb{Z}$ *and let* $b \in \mathbb{N}$, $b \geqslant 2$. *Then the linear congruence* $ax \equiv c \mod b$ *is solvable if and only if* $\gcd(a, b)$ *divides* c. *Moreover, if* $d = \gcd(a, b)$ *and* $d|c$ *then there are precisely* d *solutions in* $\mathbb{Z}_b$ *for* $ax \equiv c \mod b$.

Linear Congruences II

Theorem 1

Let $a, c \in \mathbb{Z}$ *and let* $b \in \mathbb{N}$, $b \geqslant 2$. *Then the linear congruence* $ax \equiv c \mod b$ *is solvable if and only if* $\gcd(a, b)$ *divides* c. *Moreover, if* $d = \gcd(a, b)$ *and* $d|c$ *then there are precisely* d *solutions in* $\mathbb{Z}_b$ *for* $ax \equiv c \mod b$.

Proof. First, let $d = \gcd(a, b)$ and let us assume that $d|c$. Then we consider $\tilde{a} = a/d$, $\tilde{b} = b/d$, $\tilde{c} = c/d$, and $\tilde{a}x \equiv \tilde{c} \mod \tilde{b}$.

Linear Congruences III

Now, $\gcd(\tilde{a}, \tilde{b}) = 1$, thus there is a y such that

$$\tilde{a}y \equiv 1 \mod \tilde{b}\,. \tag{1}$$

Consequently, multiplying (1) with $\tilde{c}$ yields

$$\begin{aligned} \tilde{a}y\tilde{c} &\equiv \tilde{c} \mod \tilde{b} \\ \tilde{a}x_0 &\equiv \tilde{c} \mod \tilde{b}\,, \end{aligned} \tag{2}$$

where $x_0 = y\tilde{c}$.

Linear Congruences III

Now, $\gcd(\tilde{a}, \tilde{b}) = 1$, thus there is a y such that

$$\tilde{a}y \equiv 1 \mod \tilde{b}\,. \tag{1}$$

Consequently, multiplying (1) with $\tilde{c}$ yields

$$\begin{aligned} \tilde{a}y\tilde{c} &\equiv \tilde{c} \mod \tilde{b} \\ \tilde{a}x_0 &\equiv \tilde{c} \mod \tilde{b}\,, \end{aligned} \tag{2}$$

where $x_0 = y\tilde{c}$. Hence, there is a $k \in \mathbb{Z}$ such that

$$k\tilde{b} = \tilde{a}x_0 - \tilde{c}\,.$$

Multiplying both sides by d directly yields

$$\begin{aligned} k\tilde{b}d &= \tilde{a}dx_0 - \tilde{c}d \\ kb &= ax_0 - c \end{aligned}$$

but this means nothing else than $ax_0 \equiv c \mod b$.
Consequently, x_0 is also a solution of $ax \equiv c \mod b$.

Linear Congruences IV

The remaining $(d-1)$ solutions of $ax \equiv c \mod b$ are obtained by setting $x_j = x_0 + j\tilde{b}$ for $j = 1, \ldots, d-1$.
Clearly, $x_0 < x_0 + \tilde{b} < \cdots < x_0 + (d-1)\tilde{b}$. Therefore,
$x_0, \ldots, x_0 + (d-1)\tilde{b}$ are pairwise incongruent modulo b.

Linear Congruences IV

The remaining $(d-1)$ solutions of $ax \equiv c \mod b$ are obtained by setting $x_j = x_0 + j\tilde{b}$ for $j = 1, \ldots, d-1$.
Clearly, $x_0 < x_0 + \tilde{b} < \cdots < x_0 + (d-1)\tilde{b}$. Therefore,
$x_0, \ldots, x_0 + (d-1)\tilde{b}$ are pairwise incongruent modulo b.
Since $j\tilde{b} \equiv 0 \mod \tilde{b}$ for all $j \in \mathbb{Z}$, we also have

$$\tilde{a}(x_0 + j\tilde{b}) \equiv \tilde{c} \mod \tilde{b} \,,$$

and thus there are k_j, $j = 1, \ldots, d-1$, such that

$$k_j \tilde{b} = \tilde{a}(x_0 + j\tilde{b}) - \tilde{c} \,. \tag{3}$$

Linear Congruences IV

The remaining $(d-1)$ solutions of $ax \equiv c \mod b$ are obtained by setting $x_j = x_0 + j\tilde{b}$ for $j = 1, \ldots, d-1$.
Clearly, $x_0 < x_0 + \tilde{b} < \cdots < x_0 + (d-1)\tilde{b}$. Therefore, $x_0, \ldots, x_0 + (d-1)\tilde{b}$ are pairwise incongruent modulo b.
Since $j\tilde{b} \equiv 0 \mod \tilde{b}$ for all $j \in \mathbb{Z}$, we also have

$$\tilde{a}(x_0 + j\tilde{b}) \equiv \tilde{c} \mod \tilde{b} ,$$

and thus there are k_j, $j = 1, \ldots, d-1$, such that

$$k_j\tilde{b} = \tilde{a}(x_0 + j\tilde{b}) - \tilde{c} . \tag{3}$$

Multiplying both sides of Equality (3) by d gives:

$$k_j b = a(x_0 + j\tilde{b}) - c ,$$

which again directly implies $a(x_0 + j\tilde{b}) \equiv c \mod b$. Thus, $x_0, x_0 + \tilde{b}, \ldots, x_0 + (d-1)\tilde{b}$ are all solutions of $ax \equiv c \mod b$.

Linear Congruences V

It remains to show that there are no other solutions.

Linear Congruences V

It remains to show that there are no other solutions.

Suppose the converse; i.e., there is a z such that

$$
\begin{aligned}
az &\equiv c \mod b & (4)\\
z &\not\equiv x_0 + j\tilde{b} \mod b \quad \text{for all } j = 0, \ldots, d-1\,. & (5)
\end{aligned}
$$

Linear Congruences V

It remains to show that there are no other solutions.

Suppose the converse; i.e., there is a z such that

$$\begin{aligned} az &\equiv c \mod b && (4)\\ z &\not\equiv x_0 + j\tilde{b} \mod b \quad \text{for all } j = 0, \ldots, d-1\,. && (5)\end{aligned}$$

Now, (4) implies $\tilde{a}z \equiv \tilde{c} \mod \tilde{b}$ and since $\gcd(\tilde{a}, \tilde{b}) = 1$, by Equation (2), we have

$$z \equiv x_0 \mod \tilde{b}\,.$$

Therefore, $z = x_0 + \ell\tilde{b}$. Finally, since $d\tilde{b} = b$, we can conclude that $\ell \in \{0, \ldots, d-1\}$, a contradiction to (5). Consequently, there are precisely d different solutions of $ax \equiv c \mod b$.

Linear Congruences VI

Second, let us assume that $ax \equiv c \mod b$ is solvable.

We have to show that $\gcd(a, b)$ divides c.

Linear Congruences VI

Second, let us assume that $ax \equiv c \mod b$ is solvable.

We have to show that $\gcd(a, b)$ divides c.

Let z be a solution of $ax \equiv c \mod b$, i.e., we have

$$az \equiv c \mod b\,.$$

Thus, there must be a $k \in \mathbb{Z}$ such that $kb = az - c$. But this means $kb - az = -c$ and consequently $\gcd(a, b)$ divides c. $\blacksquare$

Linear Congruences VII

Corollary 1

Let $b \in \mathbb{N}$, $b \geqslant 2$, *and let* $a, c \in \mathbb{Z}$. *If* $\gcd(a, b) = 1$ *then the linear congruence* $ax \equiv c \mod b$ *has a unique solution modulo* b.

Linear Congruences VII

Corollary 1

Let $b \in \mathbb{N}$, $b \geqslant 2$, *and let* $a, c \in \mathbb{Z}$. *If* $\gcd(a, b) = 1$ *then the linear congruence* $ax \equiv c \mod b$ *has a unique solution modulo* b.

Exercise 1. *Determine the complexity of computing all solutions of* $ax \equiv c \mod b$ *in dependence on the length of the input* $a, c \in \mathbb{Z}$ *and* $b \in \mathbb{N}$, $b \geqslant 2$.

Linear Congruences VII

Corollary 1

Let $b \in \mathbb{N}$, $b \geqslant 2$, *and let* $a, c \in \mathbb{Z}$. *If* $\gcd(a, b) = 1$ *then the linear congruence* $ax \equiv c \mod b$ *has a unique solution modulo* b.

Exercise 1. *Determine the complexity of computing all solutions of* $ax \equiv c \mod b$ *in dependence on the length of the input* $a, c \in \mathbb{Z}$ *and* $b \in \mathbb{N}$, $b \geqslant 2$.

Next, we should apply our knowledge about linear congruences to the problem of computing all integer solutions of *linear Diophantine equations*, i.e., equations of the form $ax + by = c$ for $a, b, c \in \mathbb{Z}$. This is left as an exercise.

Modular Exponentiation I

Modular exponentiation is formally defined as follows:

Modular Exponentiation

Input: Modulus $m \in \mathbb{N}$, $m \geqslant 2$, and $a \in \mathbb{Z}_m^*$ as well as $x \in \mathbb{N}$.

Problem: Compute the $y \in \{0, 1, \ldots, m-1\}$ such that
$$y \equiv a^x \mod m.$$

Note that we cannot compute a^x efficiently for n bit numbers a and x, since the output would have a length exponential in the length of the input.

Modular Exponentiation II

Theorem 2

Modular exponentiation can be computed in time $O(\max\{\log a, \log m, \log x\}^3)$.

Modular Exponentiation II

Theorem 2

Modular exponentiation can be computed in time $O(\max\{\log a, \log m, \log x\}^3)$.

Proof. Let $x = \sum_{i=0}^{k} x_i 2^{k-i}$ where $x_i \in \{0, 1\}$, i.e., x_i are the digits of x in binary notation. Then, the following procedure computes $a^x \mod m$:

Procedure EXP: "Set $y_0 = 1$
For $i = 0$ to k do
If $x_i = 0$ then $y_{i+1} := y_i^2 \mod m$;
If $x_i = 1$ then $y_{i+1} := a \cdot y_i^2 \mod m$;
Output y_{k+1}."

Modular Exponentiation III

Claim A. Procedure EXP computes y correctly.
It suffices to show that

$$y_{k+1} \equiv a^x \mod m \quad \text{for all numbers } x \text{ having } k+1 \text{ bits.}$$

We prove Claim A by induction on k.
For $k = 0$ we distinguish the cases $x = 0$ and $x = 1$.
If $x = 0$, then $y_1 = 1^2 = 1 \equiv a^0 \mod m$, and thus correct.
If $x = 1$, then $y_1 = a \cdot 1^2 = a \equiv a^1 \mod m$, and hence again correct.
Thus, the induction basis is shown.

Modular Exponentiation IV

Assume the induction hypothesis for k, i.e.,

$$y_{k+1} \equiv a^x \mod m \text{ for all numbers } x \text{ having } k+1 \text{ bits.}$$

The induction step is done from $k+1$ to $k+2$ bits.

Let $x = x_0 \ldots x_k x_{k+1}$. We may write $x = 2(x_0 \cdots x_k) + x_{k+1}$, and obtain

Modular Exponentiation IV

Assume the induction hypothesis for k, i.e.,

$$y_{k+1} \equiv a^x \mod m \text{ for all numbers } x \text{ having } k+1 \text{ bits.}$$

The induction step is done from $k+1$ to $k+2$ bits.
Let $x = x_0 \ldots x_k x_{k+1}$. We may write $x = 2(x_0 \cdots x_k) + x_{k+1}$, and obtain

$$\begin{aligned} a^x &= a^{2(x_0 \cdots x_k)+x_{k+1}} = a^{2(x_0 \cdots x_k)} \cdot a^{x_{k+1}} \equiv (a^{x_0 \cdots x_k})^2 \cdot a^{x_{k+1}} \\ &\equiv y_{k+1}^2 a^{x_{k+1}} \mod m\,. \end{aligned}$$

The latter congruence is due to the induction hypothesis.
Consequently, if $x_{k+1} = 0$ then $y_{k+2} \equiv y_{k+1}^2 \mod m$, and thus correct.

Modular Exponentiation IV

Assume the induction hypothesis for k, i.e.,

$$y_{k+1} \equiv a^x \mod m \text{ for all numbers } x \text{ having } k+1 \text{ bits.}$$

The induction step is done from $k+1$ to $k+2$ bits.
Let $x = x_0 \ldots x_k x_{k+1}$. We may write $x = 2(x_0 \cdots x_k) + x_{k+1}$, and obtain

$$\begin{aligned} a^x &= a^{2(x_0 \cdots x_k)+x_{k+1}} = a^{2(x_0 \cdots x_k)} \cdot a^{x_{k+1}} \equiv (a^{x_0 \cdots x_k})^2 \cdot a^{x_{k+1}} \\ &\equiv y_{k+1}^2 a^{x_{k+1}} \mod m\,. \end{aligned}$$

The latter congruence is due to the induction hypothesis. Consequently, if $x_{k+1} = 0$ then $y_{k+2} \equiv y_{k+1}^2 \mod m$, and thus correct. Finally, if $x_{k+1} = 1$ then $a^{x_{k+1}} = a$, and hence $y_{k+2} \equiv a \cdot y_{k+1}^2 \mod m$ which is again correct.

Modular Exponentiation V

Procedure *EXP* computes at most $2\lceil \log x \rceil$ many products modulo m over numbers from $\mathbb{Z}_m$. Thus, the Procedure EXP takes at most time cubic in the lengths of a, m, x. $\blacksquare$

Modular Exponentiation VI

Example: Calculate $3^{67} \mod 23$

$67 = 1000011$; Thus we obtain: $y_0 = 1$, and

$$
\begin{aligned}
y_1 &\equiv 3 \mod 23 \\
y_2 &\equiv 3^2 \equiv 9 \mod 23 \\
y_3 &\equiv 9^2 \equiv 12 \mod 23 \\
y_4 &\equiv 12^2 \equiv 6 \mod 23 \\
y_5 &\equiv 6^2 \equiv 13 \mod 23 \\
y_6 &\equiv 3 \cdot 13^2 \equiv 1 \mod 23 \\
y_7 &\equiv 3 \cdot 1^2 \equiv 3 \mod 23
\end{aligned}
$$

This was much easier than computing

$3^{67} = 92709463147897837085761925410587$

$= 4030846223821645090685301104808 \cdot 23 + 3$

Remark

The latter theorem shows that we can exponentiate efficiently modulo m, but what about the inverse operations? Finding discrete roots of numbers modulo m appears little less tractable, if m is prime or if the prime factorization of m is known.

In the general case, the problem of taking discrete roots seems sufficiently intractable that is has been proposed as the basis of the RSA public key cryptosystem.

Remark

The latter theorem shows that we can exponentiate efficiently modulo m, but what about the inverse operations? Finding discrete roots of numbers modulo m appears little less tractable, if m is prime or if the prime factorization of m is known.

In the general case, the problem of taking discrete roots seems sufficiently intractable that is has been proposed as the basis of the RSA public key cryptosystem.

The other inverse operation of modular exponentiation is finding discrete logarithms and defined below (cf. Definition 2).

Discrete Roots

Formally, the problem of taking discrete roots is defined as follows:

Discrete Roots

Formally, the problem of taking discrete roots is defined as follows:

Discrete Roots
Input: Modulus $m \in \mathbb{N}$, $a \in \mathbb{Z}_m^*$, and $r \in \mathbb{N}$.

Problem: Compute the solutions of $x^r \equiv a \mod m$ provided they exist or output "there are no solutions."

Euler's phi-Function I

We continue to recall basic number theory to the extend needed for designing our main algorithms. Let $m \in \mathbb{N}^+$; by $\varphi(m) =_{df} |\mathbb{Z}_m^*|$ we denote *Euler's totient function (phi-function)*.

Euler's phi-Function I

We continue to recall basic number theory to the extend needed for designing our main algorithms. Let $m \in \mathbb{N}^+$; by $\varphi(m) =_{df} |\mathbb{Z}_m^*|$ we denote *Euler's totient function (phi-function)*.

Definition 1

A function $f\colon \mathbb{N} \to \mathbb{N}$ is said to be *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$ whenever $\gcd(m, n) = 1$.

Euler's phi-Function I

We continue to recall basic number theory to the extend needed for designing our main algorithms. Let $m \in \mathbb{N}^+$; by $\varphi(m) =_{df} |\mathbb{Z}_m^*|$ we denote *Euler's totient function (phi-function)*.

Definition 1

A function $f\colon \mathbb{N} \to \mathbb{N}$ is said to be *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$ whenever $\gcd(m, n) = 1$.

The following theorem summarizes some well-known facts:

Theorem 3

(1) $\varphi(mn) = \varphi(m)\varphi(n)$ *if* $\gcd(m, n) = 1$,

(2) $\varphi(p^k) = p^{k-1}(p-1)$ *if* p *is prime and* $k \in \mathbb{N}^+$,

(3) $\varphi(p) = p - 1$ *if and only if* p *is prime.*

For the proof we refer to the book.

Euler's phi-Function II

Now we are in a position to show another important property of Euler's phi-function.

Theorem 4

For all $n \in \mathbb{N}^+$ *we have* $\sum_{d|n} \varphi(d) = n$.

Euler's phi-Function II

Now we are in a position to show another important property of Euler's phi-function.

Theorem 4

For all $n \in \mathbb{N}^+$ *we have* $\sum\limits_{d|n} \varphi(d) = n$.

Proof. First, we define $f(n) =_{df} \sum\limits_{d|n} \varphi(d)$ and show f to be multiplicative. Clearly, we have $f(1) = 1$. Now, let $m, n \in \mathbb{N}^+$ be such that $\gcd(m, n) = 1$. Consider any divisor d of mn. Since $\gcd(m, n) = 1$, there are uniquely determined numbers d_1, d_2 such that $d = d_1 d_2$ and $d_1|m$ and $d_2|n$. Thus, we have $\gcd(d_1, d_2) = 1$. By Theorem 3, we obtain $\varphi(d) = \varphi(d_1)\varphi(d_2)$.

Euler's phi-Function III

Taking into account that we get all divisors d of mn by taking all pairs (d_1, d_2), where $d_1|m$ and $d_2|n$, we conclude

$$\begin{aligned} f(mn) &= \sum_{d_1|m} \sum_{d_2|n} \varphi(d_1)\varphi(d_2) \\ &= \left(\sum_{d_1|m} \varphi(d_1)\right)\left(\sum_{d_2|n} \varphi(d_2)\right) \\ &= f(m)f(n)\,. \end{aligned}$$

Hence, f is multiplicative.

Euler's phi-Function IV

Second, since f is multiplicative, for showing the theorem it suffices to determine the value of f for prime powers p^k. The divisors of p^k are p^ℓ for $\ell = 0, \ldots, k$. Consequently, by Theorem 3 we obtain

$$f(p^k) = \sum_{\ell=0}^{k} \varphi(p^\ell) = 1 + \sum_{\ell=1}^{k} \left(p^\ell - p^{\ell-1}\right) = p^k . \qquad (6)$$

Finally, let $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ be the prime factorization of n. Then, by Equation (6), we have $f(n) = \prod_{j=1}^{m} f(p_j^{k_j}) = n$. ∎

Towards Discrete Roots and Primality Testing I

For dealing with discrete roots and with primality tests, we need more insight into the structure of the group $\mathbb{Z}_p^*$, where p is prime. That is, we aim to show that $\mathbb{Z}_p^*$ is always a cyclic group. For preparing this result, we need the following lemma:

Towards Discrete Roots and Primality Testing I

For dealing with discrete roots and with primality tests, we need more insight into the structure of the group $\mathbb{Z}_p^*$, where p is prime. That is, we aim to show that $\mathbb{Z}_p^*$ is always a cyclic group. For preparing this result, we need the following lemma:

Lemma 1

If p is prime and $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ is such that $f(b) \not\equiv 0 \mod p$ for some b, then $f(x) \equiv 0 \mod p$ has at most n distinct solutions modulo p.

The proof is provided in the book.

Back to Finite Groups

We continue with an important property of all finite groups.

Theorem 5

If $(G, \circ)$ is a finite group, then every element of G has finite order.

Back to Finite Groups

We continue with an important property of all finite groups.

Theorem 5

If $(G, \circ)$ is a finite group, then every element of G has finite order.

Proof. Let $a \in G$ be arbitrarily fixed, and let e be the neutral element of $(G, \circ)$. Consider the elements a, a^2, $a^3, \ldots$. Since G is finite, there must exist $k, \ell \in \mathbb{N}^+$ such that $k > \ell$ and $a^k = a^\ell$. Since G is a group, the inverse b of a^ℓ exists and since the inverse is uniquely determined, it must be equal to $a^{-\ell}$. Therefore, we obtain $a^k \circ a^{-\ell} = a^\ell \circ a^{-\ell} = e$. This implies that $a^{k-\ell} = e$. Hence, there exists an $m \in \mathbb{N}^+$ such that $a^m = e$, i.e., $m = k - \ell$. Consequently, the must be a least such number $n \in \mathbb{N}^+$ satisfying $a^n = e$, and so $n = \mathrm{ord}(a)$. ∎

Towards Discrete Roots and Primality Testing II

Theorem 6

If p is prime then $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

Towards Discrete Roots and Primality Testing II

Theorem 6

If p is prime then $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

Proof. Let p prime. By Theorem 3 we already know that $\varphi(p) = |\mathbb{Z}_p^*| = p-1$; thus $\mathbb{Z}_p^*$ has order $p-1$. In order to see that $\mathbb{Z}_p^*$ is cyclic, we have to show that it has an element of order $p-1$. This is achieved by counting elements of different order. Let d be any positive integer such that $d|(p-1)$. Define

$$S_d \quad =_{df} \quad \{a \in \mathbb{Z}_p^* \mid \operatorname{ord}(a) = d\}\,. \tag{7}$$

Towards Discrete Roots and Primality Testing II

Theorem 6

If p is prime then $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

Proof. Let p prime. By Theorem 3 we already know that $\varphi(p) = |\mathbb{Z}_p^*| = p-1$; thus $\mathbb{Z}_p^*$ has order $p-1$. In order to see that $\mathbb{Z}_p^*$ is cyclic, we have to show that it has an element of order $p-1$. This is achieved by counting elements of different order. Let d be any positive integer such that $d|(p-1)$. Define

$$S_d =_{df} \{a \in \mathbb{Z}_p^* \mid \operatorname{ord}(a) = d\} . \tag{7}$$

These sets S_d partition $\mathbb{Z}_p^*$, so we have

$$\sum_{d|(p-1)} |S_d| = |\mathbb{Z}_p^*| = p - 1 . \tag{8}$$

Towards Discrete Roots and Primality Testing III

Fix d such that $d|(p-1)$. We show that either $|S_d| = 0$ or $|S_d| = \varphi(d)$. Suppose $S_d \neq \emptyset$, and choose some $a \in S_d$. Then $a, a^2, \ldots, a^d$ are all distinct modulo p and each one is a solution of $x^d \equiv 1 \mod p$. By Lemma 1 above, this equation has at most d solutions modulo p, so these are all of the solutions. Consequently, $S_d \subseteq \{a^k \mid 1 \leqslant k \leqslant d\}$.

Towards Discrete Roots and Primality Testing III

Fix d such that $d|(p-1)$. We show that either $|S_d| = 0$ or $|S_d| = \varphi(d)$. Suppose $S_d \neq \emptyset$, and choose some $a \in S_d$. Then $a, a^2, \ldots, a^d$ are all distinct modulo p and each one is a solution of $x^d \equiv 1 \mod p$. By Lemma 1 above, this equation has at most d solutions modulo p, so these are all of the solutions. Consequently, $S_d \subseteq \{a^k \mid 1 \leqslant k \leqslant d\}$.
Now, fix $k \in \{1, \ldots, d\}$. If $\gcd(k, d) = \ell > 1$, then $(a^k)^{d/\ell} = (a^{k/\ell})^d \equiv 1 \mod p$, so a^k has order less than d, and therefore $a^k \notin S_d$.

Towards Discrete Roots and Primality Testing III

Fix d such that $d|(p-1)$. We show that either $|S_d| = 0$ or $|S_d| = \varphi(d)$. Suppose $S_d \neq \emptyset$, and choose some $a \in S_d$. Then $a, a^2, \ldots, a^d$ are all distinct modulo p and each one is a solution of $x^d \equiv 1 \mod p$. By Lemma 1 above, this equation has at most d solutions modulo p, so these are all of the solutions. Consequently, $S_d \subseteq \{a^k \mid 1 \leqslant k \leqslant d\}$.

Now, fix $k \in \{1, \ldots, d\}$. If $\gcd(k, d) = \ell > 1$, then $(a^k)^{d/\ell} = (a^{k/\ell})^d \equiv 1 \mod p$, so a^k has order less than d, and therefore $a^k \notin S_d$.

If $\gcd(k, d) = 1$, then there exists ℓ such that $k\ell \equiv 1 \mod d$. Hence, $a^{k\ell} \equiv a \mod p$. Furthermore, for any $e \in \{1, \ldots, d-1\}$ we have

$$((a^k)^e)^\ell \equiv a^e \not\equiv 1 \mod p,$$

so a^k is of order d, i.e., $a^k \in S_d$.

Towards Discrete Roots and Primality Testing IV

Thus, we have shown

$$S_d = \{a^k \mid 1 \leqslant k \leqslant d,\ \gcd(k, d) = 1\},$$

and consequently $|S_d| = \varphi(d)$.

Towards Discrete Roots and Primality Testing IV

Thus, we have shown

$$S_d = \{a^k \mid 1 \leqslant k \leqslant d,\ \gcd(k, d) = 1\}\,,$$

and consequently $|S_d| = \varphi(d)$.

Now suppose that for some d such that $d|(p-1)$, $S_d = \emptyset$. Then

$$\sum_{d|(p-1)} |S_d| < \sum_{d|(p-1)} \varphi(d)\,. \tag{9}$$

Towards Discrete Roots and Primality Testing IV

Thus, we have shown

$$S_d = \{a^k \mid 1 \leqslant k \leqslant d,\ \gcd(k,d) = 1\}\,,$$

and consequently $|S_d| = \varphi(d)$.
Now suppose that for some d such that $d|(p-1)$, $S_d = \emptyset$. Then

$$\sum_{d|(p-1)} |S_d| < \sum_{d|(p-1)} \varphi(d)\,. \tag{9}$$

By Theorem 4, we know that

$$\sum_{d|(p-1)} \varphi(d) = p - 1\,.$$

Thus, (9) would give a contradiction to Eq. (8). Hence, for each d with $d|(p-1)$ we have $|S_d| = \varphi(d)$. This proves the theorem. Moreover, the number of elements of order $p-1$ is $\varphi(p-1)$. ∎

Towards Discrete Roots and Primality Testing V

As we have seen, if p is prime then $\mathbb{Z}_p^*$ is cyclic. Every element g of order $p-1$ is called a *generator* of $\mathbb{Z}_p^*$. Hence, for every $a \in \mathbb{Z}_p^*$ there exists exactly one $x \in \{1, 2, \ldots, p\}$ such that $a = g^x$. We refer to x as the *discrete logarithm* of a with respect to g, and denote it by $x = \mathrm{dlog}_g\, a$.

Towards Discrete Roots and Primality Testing V

As we have seen, if p is prime then $\mathbb{Z}_p^*$ is cyclic. Every element g of order $p-1$ is called a *generator* of $\mathbb{Z}_p^*$. Hence, for every $a \in \mathbb{Z}_p^*$ there exists exactly one $x \in \{1, 2, \ldots, p\}$ such that $a = g^x$. We refer to x as the *discrete logarithm* of a with respect to g, and denote it by $x = \mathrm{dlog}_g\, a$.

Not that the condition p being prime is sufficient but not necessary for the cyclicity of $\mathbb{Z}_p^*$, since one can prove the following:

Theorem 7

$\mathbb{Z}_n^*$ is cyclic if and only if n is 1, 2, 4, p^k, or $2p^k$ for some odd prime number p and $k \in \mathbb{N}^+$.

Towards Discrete Roots and Primality Testing VI

So, it is appropriate to generalize the definition of discrete logarithms.

Definition 2 (Discrete Logarithm)

Let $n \in \mathbb{N}^+$ be such that $\mathbb{Z}_n^*$ is cyclic. Furthermore, let g be a generator of $\mathbb{Z}_n^*$ and let $a \in \mathbb{Z}_n^*$. Then there exists a unique number $z \in \{1, \ldots, \varphi(n)\}$ such that $g^z \equiv a \mod n$. This z is called the *discrete logarithm* of a modulo n to the base g and denoted by $\mathrm{dlog}_g\, a$.

Towards Discrete Roots and Primality Testing VI

So, it is appropriate to generalize the definition of discrete logarithms.

Definition 2 (Discrete Logarithm)

Let $n \in \mathbb{N}^+$ be such that $\mathbb{Z}_n^*$ is cyclic. Furthermore, let g be a generator of $\mathbb{Z}_n^*$ and let $a \in \mathbb{Z}_n^*$. Then there exists a unique number $z \in \{1, \ldots, \varphi(n)\}$ such that $g^z \equiv a \mod n$. This z is called the *discrete logarithm* of a modulo n to the base g and denoted by $\mathrm{dlog}_g\, a$.

Now, let p be a prime and let g be any generator for $\mathbb{Z}_p^*$. Then we obviously have $g^{p-1} \equiv 1 \mod p$. The latter property is, however, not restricted to generators as the following theorem shows:

Euler's Theorem

Theorem 8 (Euler's Theorem)

Let $n \in \mathbb{N}$, $n \geqslant 2$; *then* $a^{\varphi(n)} \equiv 1 \mod n$ *for all* $a \in \mathbb{Z}_n^*$.

Euler's Theorem

Theorem 8 (Euler's Theorem)

Let $n \in \mathbb{N}$, $n \geqslant 2$; *then* $a^{\varphi(n)} \equiv 1 \mod n$ *for all* $a \in \mathbb{Z}_n^*$.

Proof. Recall that $\varphi(m) = |\mathbb{Z}_m^*|$, i.e., $\varphi(m)$ is the order of the group $\mathbb{Z}_m^*$. Let $a \in \mathbb{Z}_m^*$ be arbitrarily fixed. By Theorem 5, we know that $\operatorname{ord}(a)$ is finite, say k. Furthermore, $S = \{a^n \mid n = 1, \ldots, k\}$ is a subgroup of $\mathbb{Z}_m^*$. By Corollary 3.1 we conclude that $k|\varphi(m)$. Thus, there is an $\ell \in \mathbb{N}^+$ such that $\varphi(m) = k\ell$. Consequently,

$$a^{\varphi(m)} \equiv a^{k\ell} \equiv (a^k)^\ell \equiv 1 \mod m.$$

∎

Fermat's Little Theorem

Theorem 8 covers the following important special case which was first discovered by Pierre de Fermat:

Theorem 9 (Fermat's Little Theorem)

Let p *be a prime. Then* $a^{p-1} \equiv 1 \mod p$ *for all* $a \in \mathbb{Z}_p^*$.

Proof. Since $\varphi(p) = p - 1$, the assertion directly follows from Theorem 8. ∎

Fermat's Little Theorem

Theorem 8 covers the following important special case which was first discovered by Pierre de Fermat:

Theorem 9 (Fermat's Little Theorem)

Let p *be a prime. Then* $a^{p-1} \equiv 1 \mod p$ *for all* $a \in \mathbb{Z}_p^*$.

Proof. Since $\varphi(p) = p - 1$, the assertion directly follows from Theorem 8.

Next, we turn our attention to testing primality.

Testing Primality

Input: Any natural number $n \geqslant 2$.

Problem: Decide whether or not n is prime.

Pseudo Primes I

Though *testing primality* is a very old problem, no deterministic algorithm has been known that runs in time polynomial in the length of the input until 2002. Then Agrawal, Kayal and Saxena succeeded to provide an affirmative answer to this very long standing open problem.

Clearly, one could get a deterministic polynomial time algorithm for testing primality, if the converse of Theorem 9 were true. Unfortunately, it is not. We continue by figuring out why the converse of Theorem 9 is not true.

Pseudo Primes II

Definition 3 (Pseudo Primes)

Let $n \in \mathbb{N}$ be an odd composite number, and let $b \in \mathbb{N}$ such that $\gcd(b, n) = 1$. Then n is said to be *pseudo-prime to the base* b if $b^{n-1} \equiv 1 \mod n$.

For example, $n = 91$ is a pseudo-prime to the base 3, since $91 = 7 \cdot 13$ and, furthermore, $3^{90} \equiv 1 \mod 91$ (note that $3^6 = 729 = 8 \cdot 91 + 1 \equiv 1 \mod 91$).

But 91 is not a pseudo-prime to the base 2, since $2^{90} \equiv 64 \mod 91$.

Pseudo Primes III

The following theorem summarizes important properties of pseudo-primes:

Theorem 10

Let $n \in \mathbb{N}$ be an odd composite number. Then we have

(1) n *is pseudo-prime to the base* b *with* $\gcd(b, n) = 1$ *if and only if the order* d *of* b *in* $\mathbb{Z}_n^*$ *divides* $n - 1$.

(2) *If* n *is pseudo-prime to the bases* b_1 *and* b_2 *such that* $\gcd(b_1, n) = 1$ *and* $\gcd(b_2, n) = 1$, *then* n *is also pseudo-prime to the bases* $b_1 b_2$, $b_1 b_2^{-1}$, *and* $b_1^{-1} b_2$.

(3) *If there is a* $b \in \mathbb{Z}_n^*$ *satisfying* $b^{n-1} \not\equiv 1 \mod n$, *then*

$$\left|\{b \in \mathbb{Z}_n^* \mid b^{n-1} \not\equiv 1 \mod n\}\right| \geqslant \frac{\varphi(n)}{2} .$$

Pseudo Primes IV

Proof. First, we show (1). The necessity can be seen as follows: Let n be pseudo-prime to the base b with $\gcd(b, n) = 1$. Then, we have $b^{n-1} \equiv 1 \mod n$. Let d be the smallest positive number for which $b^d \equiv 1 \mod n$. Suppose, $n - 1 = kd + r$ with $0 < r < d$. Then we would get

$$b^{n-1} \equiv b^{kd+r} \equiv b^{kd}b^r \equiv \left(b^d\right)^k b^r \equiv b^r \not\equiv 1 \mod n\,,$$

a contradiction. Hence, d must divide $n - 1$.

Pseudo Primes IV

Proof. First, we show (1). The necessity can be seen as follows: Let n be pseudo-prime to the base b with $\gcd(b, n) = 1$. Then, we have $b^{n-1} \equiv 1 \mod n$. Let d be the smallest positive number for which $b^d \equiv 1 \mod n$. Suppose, $n - 1 = kd + r$ with $0 < r < d$. Then we would get

$$b^{n-1} \equiv b^{kd+r} \equiv b^{kd}b^r \equiv \left(b^d\right)^k b^r \equiv b^r \not\equiv 1 \mod n\,,$$

a contradiction. Hence, d must divide $n - 1$.

For the sufficiency, assume d divides $n - 1$. Thus, $n - 1 = kd$ for some k. Hence, $b^{n-1} \equiv (b^d)^k \equiv 1^k \equiv 1 \mod n$. Consequently, n is pseudo-prime to the base b.

Pseudo Primes V

Assertion (2) is left as an exercise. Finally, we prove (3). Let $b \in \mathbb{Z}_n^*$ be such that $b^{n-1} \not\equiv 1 \mod n$. Let $\{b_1, \ldots, b_s\}$ all the bases for which n is pseudo-prime, i.e.,

$$b_i^{n-1} \equiv 1 \mod n \text{ for all } i = 1, \ldots, s\,. \tag{10}$$

Pseudo Primes V

Assertion (2) is left as an exercise. Finally, we prove (3). Let $b \in \mathbb{Z}_n^*$ be such that $b^{n-1} \not\equiv 1 \mod n$. Let $\{b_1, \ldots, b_s\}$ all the bases for which n is pseudo-prime, i.e.,

$$b_i^{n-1} \equiv 1 \mod n \text{ for all } i = 1, \ldots, s\,. \tag{10}$$

Since

$$b^{n-1} \equiv c \not\equiv 1 \mod n \tag{11}$$

for some $c \in \mathbb{Z}_n^*$, we obtain, by multiplying (10) with (11), where $i = 1, \ldots, s$ that

$$c \equiv b_i^{n-1} b^{n-1} \equiv (b_i b)^{n-1} \mod n\,.$$

Pseudo Primes V

Assertion (2) is left as an exercise. Finally, we prove (3). Let $b \in \mathbb{Z}_n^*$ be such that $b^{n-1} \not\equiv 1 \mod n$. Let $\{b_1, \ldots, b_s\}$ all the bases for which n is pseudo-prime, i.e.,

$$b_i^{n-1} \equiv 1 \mod n \text{ for all } i = 1, \ldots, s\,. \tag{10}$$

Since

$$b^{n-1} \equiv c \not\equiv 1 \mod n \tag{11}$$

for some $c \in \mathbb{Z}_n^*$, we obtain, by multiplying (10) with (11), where $i = 1, \ldots, s$ that

$$c \equiv b_i^{n-1} b^{n-1} \equiv (b_i b)^{n-1} \mod n\,.$$

Hence, n is not a pseudo-prime to all the bases $\{b_1 b, \ldots, b_s b\}$. Consequently, there are at least as many bases for which n is not a pseudo-prime as there are bases for which n is pseudo-prime. ∎

Pseudo Primes VI

Now, if we knew that for all odd composite numbers n there should exist at least one number $b \in \mathbb{Z}_n^*$ such that n is not a pseudo-prime to the base b, we could easily design a probabilistic polynomial time algorithm for testing primality. But again, unfortunately, there are odd composite numbers n such that $b^{n-1} \equiv 1 \mod n$ for *all* $b \in \mathbb{Z}_n^*$. These numbers are called *Carmichael numbers* (named after Robert D. Carmichael).

Pseudo Primes VI

Now, if we knew that for all odd composite numbers n there should exist at least one number $b \in \mathbb{Z}_n^*$ such that n is not a pseudo-prime to the base b, we could easily design a probabilistic polynomial time algorithm for testing primality. But again, unfortunately, there are odd composite numbers n such that $b^{n-1} \equiv 1 \mod n$ for *all* $b \in \mathbb{Z}_n^*$. These numbers are called *Carmichael numbers* (named after Robert D. Carmichael).

We need one more exercise.

Exercise 2. *Let p be a prime number. Then $\mathbb{Z}_{p^2}^*$ is cyclic.*

Furthermore, a number n is said to be *square-free* if there is no square number dividing it.

Carmichael Numbers I

Theorem 11

Let $n \in \mathbb{N}$ *be an odd composite number. Then we have*

(1) *If there is a square number* $q^2 > 1$ *dividing* n *then* n *is not a Carmichael number.*

(2) *If* n *is square-free, then* n *is Carmichael number if and only if* $(p - 1)$ *divides* $n - 1$ *for every prime* p *dividing* n.

Carmichael Numbers II

Proof. Assume any number $q^2 > 1$ dividing n, and let $p > 2$ be a prime factor of q. Since $q^2|n$, we also know that p^2 is dividing n. Moreover, by Exercise 2 we know that $\mathbb{Z}^*_{p^2}$ is cyclic.

Carmichael Numbers II

Proof. Assume any number $q^2 > 1$ dividing n, and let $p > 2$ be a prime factor of q. Since $q^2|n$, we also know that p^2 is dividing n. Moreover, by Exercise 2 we know that $\mathbb{Z}^*_{p^2}$ is cyclic. Let g be a generator of $\mathbb{Z}^*_{p^2}$. Next, we construct a number $b \in \mathbb{Z}^*_n$ such that $b^{n-1} \not\equiv 1 \mod n$. If we can do that, then n cannot be a Carmichael number.

Carmichael Numbers II

Proof. Assume any number $q^2 > 1$ dividing n, and let $p > 2$ be a prime factor of q. Since $q^2|n$, we also know that p^2 is dividing n. Moreover, by Exercise 2 we know that $\mathbb{Z}_{p^2}^*$ is cyclic. Let g be a generator of $\mathbb{Z}_{p^2}^*$. Next, we construct a number $b \in \mathbb{Z}_n^*$ such that $b^{n-1} \not\equiv 1 \mod n$. If we can do that, then n cannot be a Carmichael number.
Let $\tilde{n}$ be the product of all primes $r \neq p$ that divide n. Obviously, $\gcd(p^2, \tilde{n}) = 1$. By the Chinese remainder theorem there is a number b such that

$$\begin{aligned} b &\equiv g \mod p^2 \\ b &\equiv 1 \mod \tilde{n} \end{aligned}$$

So b is also a generator of $\mathbb{Z}_{p^2}^*$.

Carmichael Numbers III

Now we show $b \in \mathbb{Z}_n^*$ by proving $\gcd(n, b) = 1$.
Suppose the converse, i.e., $1 < d = \gcd(n, b)$.
Case 1. p divides d.
If $p|d$, we know that $p|b$ and since $p^2|(b-g)$, we additionally have $p|(b-g)$. Consequently, $p|g$, too. But this implies $g \notin \mathbb{Z}_{p^2}^*$, a contradiction. Thus, Case 1 cannot happen.

Carmichael Numbers III

Now we show $b \in \mathbb{Z}_n^*$ by proving $\gcd(n, b) = 1$.
Suppose the converse, i.e., $1 < d = \gcd(n, b)$.
Case 1. p divides d.
If $p|d$, we know that $p|b$ and since $p^2|(b - g)$, we additionally have $p|(b - g)$. Consequently, $p|g$, too. But this implies $g \notin \mathbb{Z}_{p^2}^*$, a contradiction. Thus, Case 1 cannot happen.
Case 2. p does not divide d.
Consider any prime r dividing n and d simultaneously. Then, $r \neq p$ by assumption. Hence, $r|b$, too, and moreover, $\tilde{n}|(b - 1)$ because of $b \equiv 1 \mod \tilde{n}$. But $r \neq p$, so $r|\tilde{n}$, too, and thus $r|(b - 1)$. This implies $r = 1$, a contradiction.
This proves $b \in \mathbb{Z}_n^*$.

Carmichael Numbers IV

Finally, we have to show that $b^{n-1} \not\equiv 1 \mod n$. Suppose the converse, i.e., $b^{n-1} \equiv 1 \mod n$. Since $p^2|n$, we conclude $b^{n-1} \equiv 1 \mod p^2$, too. But b is a generator of $\mathbb{Z}^*_{p^2}$. Thus, by the Theorem of Euler we get $\varphi(p^2)|(n-1)$, i.e., $p(p-1)|(n-1)$. This means in particular

$$n - 1 \equiv 0 \mod p\ .$$

On the other hand, by construction we know that $p|n$, and hence

$$n - 1 \equiv -1 \mod p\ ,$$

a contradiction. Therefore, we have proved $b^{n-1} \not\equiv 1 \mod n$ and Assertion (1) is shown.

Carmichael Numbers V

Next, we prove Assertion (2).
Sufficiency. Let $b \in \mathbb{Z}_n^*$; we have to show $b^{n-1} \equiv 1 \mod n$. Since n is square-free, it suffices to show $p | (b^{n-1} - 1)$ provided $p | n$. Assume $p | n$ and by assumption also $k(p-1) = n - 1$ for some k. By Theorem 9 we have $b^{p-1} \equiv 1 \mod p$, and consequently

$$1 \equiv 1^k \equiv (b^{p-1})^k \equiv b^{n-1} \mod p\ .$$

This holds for all prime divisors p of n; thus the sufficiency follows.

Carmichael Numbers VI

Necessity. Assume $b^{n-1} \equiv 1 \mod n$ for all $b \in \mathbb{Z}_n^*$. Now, we have to show that $(p-1)|(n-1)$ for all primes p with $p|n$. Suppose there is a prime p with $p|n$ such that $(p-1)$ does not divide $(n-1)$. Hence, there are numbers k, r such that $(n-1) = k(p-1) + r$ and $0 < r < p-1$. Now, we again construct a $b \in \mathbb{Z}_n^*$ with $b^{n-1} \not\equiv 1 \mod n$. Let g be a generator of $\mathbb{Z}_p^*$ and let $\tilde{n} = n/p$. By the Chinese remainder theorem there is a number b such that

$$b \equiv g \mod p \quad \text{and} \quad b \equiv 1 \mod \tilde{n} .$$

Consequently, b is also a generator of $\mathbb{Z}_p^*$. On the other hand,

$$b^{n-1} \equiv b^{k(p-1)+r} \equiv 1^k b^r \equiv b^r \not\equiv 1 \mod p ,$$

since b is generator. Thus, p does not divide $(b^{n-1} - 1)$, and therefore n does not divide $(b^{n-1} - 1)$, too. ∎

Carmichael Numbers VII

In order to have an example, it is now easy to see that 561 is a Carmichael number. We have just to verify that 2, 10, and 16 divide 560.

Exercise 3. *Every Carmichael number is the product of at least 3 distinct primes.*

Thank you!

Leonhard Euler

Pierre de Fermat

Robert Daniel Carmichael