Discrete Mathematics

2019~2020　(第一学期)

Department of Computer Science, East China Normal University

September 10, 2019

Chapter 2 NUMBER THEORY

素数

Definition (素数)

素数 (prime number): i) 整数, ii) 大于 1, iii) 只有 1 和自身两个正因数;
合数: i) 整数, ii) 大于 1, iii) 非素数.

Example

- 素数: $2, 3, 5, 7, 11, \ldots$;
- 合数: $4, 6, 8, 9, 10, \ldots$;
- 非素数且非合数: $1, 0, -1, -2, -3, \ldots$.

QUIZ: 求方程 $xy + 2y - 3x = 25$ 的所有整数解.

素数

Theorem

设 n 是大于 1 的整数, 它除 1 外的最小正因数 q 必为素数;
并且当 n 是合数时, $q \leq \sqrt{n}$.

用筛选法构造不超过 $n \in \mathbb{N}$ 的素数表:
从 2 到 n 的列表中, 依次删去素数 $2, 3, 5, 7, 11, \ldots$ 的倍数, 其中所需考虑的素数不大于 $\sqrt{n}$.

素数

Theorem

设 p 是素数, $n_1, n_2, \ldots, n_k \in \mathbb{N}$.
若 $p \mid n_1 \cdot n_2 \cdot \cdots \cdot n_k$, 则 $p \mid n_1, p \mid n_2, \cdots, p \mid n_k$ 其中必有一个成立.

Theorem (算术基本定理)

对于每一个正整数 $n > 1$ 都可唯一地分解为素数的幂之积 (**正整数的标准分解式**):

$$n = p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \cdots \cdot p_k^{\varepsilon_k},$$

其中 $p_1, p_2, \ldots, p_k$ 是互异的素数, $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k \in \mathbb{N}$.

Theorem

素数有无穷多个.

欧拉函数

Definition (Euler's function)

欧拉函数 $\varphi(n) : n \in \mathbb{N}$ 是记录小于 n 并与 n 互素的正整数个数.

Theorem

设 $n \in \mathbb{N}$ 有标准分解式: $n = p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \cdots \cdot p_k^{\varepsilon_k}$, 则

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \cdots \cdot (1 - \frac{1}{p_k}).$$

TIP: Prove it by the principle of inclusion–exclusion.

欧拉定理

Theorem (Euler's theorem)

若 $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, n) = 1$, 则有 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corollary (Fermat's little theorem)

设 p 为素数, $a \in \mathbb{Z}$, 且 $(a, p) = 1$, 则有 $a^{p-1} \equiv 1 \pmod{p}$.

Proof.

It follows immediately from Euler's theorem by choosing $n = p$. □

二次探测定理

Theorem (二次探测定理)

若 p 是素数, 则 $x^2 \equiv 1 \pmod{p}$ 的解为 $x \equiv 1 \pmod{p}$ 或 $x \equiv p-1 \pmod{p}$.

Proof.

$$
\begin{aligned}
& x^2 \equiv 1 \pmod{p} \\
\Longleftrightarrow \quad & (x-1)(x+1) \equiv 0 \pmod{p} \\
\Longleftrightarrow \quad & p \mid (x-1)(x+1) \\
\Longleftrightarrow \quad & x \equiv 1 \pmod{p} \text{ 或 } x \equiv p-1 \pmod{p}.
\end{aligned}
$$

□

素性探测

Testing whether a natural number is a prime number is a fundamental problem, with application to the Rivest–Shamir–Adleman public-key cryptosystem.

Theorem (Wilson's theorem)

对于任意 $n \in \mathbb{N}$, n 是素数的充分必要条件是 $(n-1)! \equiv -1 \pmod{n}$.

充分条件和必要条件.
Wilson 定理和筛法都不适用于检测大整数的素性,
尚没有高效的确定性的 (deterministic) 素性测试算法,
仅有一些非确定性的 (nondeterministic) 随机算法.

Miller–Rabin 测试

Miller–Rabin 测试

注：判定一个正整数$n(n>1)$是不是素数？没有有效的基于充分条件的算法. 可考虑借助于必要条件设计算法.

检测多个必要条件以提高可靠性,

费马小定理 + 二次探测定理,

已证明算法出错的概率小于等于 1/4,

若反复测试 k 次, 则错误概率可降低为$(\frac{1}{4})^k$.

Miller–Rabin 测试

GOAL: 测试 n 是不是素数.

若 $n > 2$ 是素数, 则 n 可表示为 $n = m \cdot 2^q + 1$, 其中 m 是奇数.

0 由费马小定理, 可得: $a^{n-1} = a^{m \cdot 2^q} \equiv 1 \pmod{n}$, 其中 $1 < a < n-1$ 是随机选取的自然数.

1 由二次探测定理, 可得:
$a^{m \cdot 2^{q-1}} \equiv 1 \pmod{n}$ 或 $a^{m \cdot 2^{q-1}} \equiv n-1 \pmod{n}$.

2 若 $a^{m \cdot 2^{q-1}} \equiv 1 \pmod{n}$, 则再由二次探测定理, 可得:
$a^{m \cdot 2^{q-2}} \equiv 1 \pmod{n}$ 或 $a^{m \cdot 2^{q-2}} \equiv n-1 \pmod{n}$.

r 依次向前递推, 即对任意的 $r(0 \le r < q-1)$, 若 $a^{2^r m} \equiv 1 (mod n)$, 则有 $a^{2^{r-1} m} \equiv 1 (mod n)$ 或 $a^{2^{r-1} m} \equiv n-1 \pmod{n}$. 如发生后者, 终止二次探测.

当 n 是素数时, 必有 $a^m (mod n) = 1$, 或上述测试序列中某一步的余数为 $n-1$.

Miller–Rabin 测试

Miller 序列: $a^{m\cdot 2^0} \mod n, a^{m\cdot 2^1} \mod n, \ldots, a^{m\cdot 2^q} \mod n$.
测试它们的值是否为:

1. $1, \ldots, 1,$
2. $*, n-1, 1, \ldots, 1, 1,$ 其中 $*$ 表示任意前缀情况.

只有在这两种情况下, n 才可能是素数. (必要条件)

Homework

令 $M = 100000, N = 1000000007$, 设你的学号为 x, 求解以下问题：

1. $p = \lfloor x/M \rfloor$, $q = x \bmod M$, 求 $r_1 = p^q \bmod N$。
2. 求最小的素数 r_2 使其满足，$r_2 \geq r_1$。

写作业时依次给出 x, r_1, r_2 的值。
例如你们助教的学号是 $x = 51164500057$, 则该题的答案是

$$51164500057 \quad 193157841 \quad 193157863$$

Hint

- 取前 7 个素数做 Miller-Rabin 测试，能够保证在输入小于3.4×10^{14}时，结果是完全正确的。
- 根据孪生素数猜想的最新研究成果，相邻两个素数之差不超过 246.