数理工学セミナー (離散数理) Day12

川上篤史

金 2

2020/1/17

Abstract

- 前回はステインのアルゴリズムを用いた gcd の計算やその拡張をしていました。
- 今回は 13 章『現実世界での応用』ということで, 前半部分の フェルマーの小定理 (Fermat's little theorem) に基づく素数判 定法に関して話します.
- 後半部分は habara くんが発表します.

目次

- ① Chapter13-1:暗号学
- ② Chapter13-2:素数判定

目次

- ① Chapter13-1:暗号学
- ② Chapter13-2:素数判定
- ③ Chapter13-3:ミラー・ラビンテスト

定義 A1:暗号方式

暗号文 Cryptogram とは、平文 $Plane_text$ をある暗号化の方法 Encryption に基づき、与えられた鍵 key_0 によって暗号化したものである.

また、暗号文は暗号化に対応する復号化の方法 Decryption 及び与えられた鍵 key_1 によって元の平文に復号される. すなわち、

Cryptogram = Encryption(key₀, Plane_text), Plane_text = Decryption(key₁, Cryptogram)

シーザー暗号 (Caesar cipher)

シーザー暗号

- アルファベットの平文の各文字をアルファベット順で何文字 かずつずらすことによって生成する.
- 何文字シフトしたのかが分かれば, 復号は逆にシフトすれば 良いので容易.
- 資料でアルファベットを『回転させる』と書いてあるが, 正しく『シフト』である。
- Encryption = Shift_on_Alphhabet, key₀ は何文字シフトするかを表す自然数 (Decryption, key₁ も同様.
- 例えば, Shift_on_Alphhabet(3, "suri love") = "vxul"

- key₀ = key₁ のとき, その暗号方式は対称であるといい, そうでないとき 非対称という.
- 対称な暗号システムでは鍵の授受のセキュリティが問題となる。

定義 A2:公開鍵暗号方式

公開鍵と秘密鍵の組 (pub, prv) を使用し, 以下の要件を満たすものを公開鍵暗号方式と呼ぶ.

- Encryption の計算は容易で Decryption の計算が困難 (鍵のサイズに対し指数時間を要する).
- トラップドアと呼ばれる追加情報を持てば *Decryption* の計算が容易となる.
- Encryption と Decryption のアルゴリズムは公開されている.

素数を利用した暗号方式の準備

- 自然数 n の素数判定の計算量について考える.
- ullet 1 以上 \sqrt{n} 以下の自然数について n を割り切るかを全探索すれば $O(\sqrt{n})$.
- 決定的な ({素数である/素数ではない}を返す)素数判定の計算量は $O(\sqrt{n})=O(2^{(\log n)/2})$.
- これは桁数 (~ log₁₀n) に対し指数時間.
- そこで, 確率的 ({素数ではない/ 不明 } を返す) だが桁数に対し多項式時間で判定できるアルゴリズムとして, 以下ではフェルマーテストについて考える.

フェルマーテスト

定理 A3

p が素数 $\Rightarrow \forall a(0 < a < p) \in \mathbb{N}, \ a^{p-1} - 1 \equiv 0 \pmod{p}$

フェルマーテスト: n は素数か?

- STEP1: n 未満の正の整数 a(証拠) を任意に取る.
- STEP2: a と n が互いに素でなければ n は合成数なので終了.
- STEP3: aⁿ⁻¹ 1 ≠ 0 (mod n) ならば, 定理 A3 の対偶より n は 素数ではないとして終了.
- STEP4: 十分な回数 STEP1, 2, 3 を繰り返す.
- STEP5: n は素数である可能性が高いとして終了.

カーマイケル数

定義 13.1

以下を満たす合成数 n > 1 をカーマイケル数 (Carmichael number) という.

 $\forall b > 1$, coprime $(b, n) \Rightarrow b^{n-1} \equiv 1 \mod n$

問題 13.1

nがカーマイケル数であるかを判定する関数を実装せよ.

問題 13.2

問題 13.1 の関数を用いて, 最初の 7 つのカーマイケル数を見つけ だせ.

カーマイケル数の判定

解答 13.1, 2

- n より大きい b については b = kn + r (r < n) と表される.
- $b^{n-1} \equiv r^{n-1} \pmod{n}$ なので結局 n 以下の b についてのみ考えればよい.
- カーマイケル数に対してフェルマーテストが必ず失敗するか と言えばそうでもない (互いに素でない証拠を見つける場合 があるため).
- 各 n に対して b を全探索して O(n²logn)
- 561, 1105, 1729, 2465, 2821, 6601, 8911, …と続く.

カーマイケル数の判定

定理:コルセルトの判定法 (Koselt Criterion)

合成数 n について, 以下の (i)(ii) は同値である.

- (i)n はカーマイケル数である.
- (ii)n は奇素数の積で表され, n の任意の素因数 p について n-1 は p-1 で割り切れる.
- (ii)⇒(i) の証明は板書します.
- (i)⇒(ii) の証明は略. CRT(中国剰余定理) を使うらしい.¹
- ullet n に対し約数列挙 $(O(\sqrt{n}))$ をして各約数について条件を確認すればよい.
- ullet これを実装すると $O(n\sqrt{n})$ だが愚直な実装の方が早い.
- エラトステネスの篩の応用で O(nloglogn) らしい.2

目次

- ① Chapter13-1:暗号学
- ② Chapter13-2:素数判定

ミラー・ラビンテスト

定理 A4

任意の素数 n と任意の整数 x(0 < x < n) について, $x^2 \equiv 1 \pmod{n} \Rightarrow x = 1$ または x = -1 が成立.

- 同様の仮定のもとで対偶: $x \neq \pm 1 \Rightarrow x^2 \not\equiv 1 \pmod{n}$) が成立.
- $\Rightarrow x \neq \pm 1$ かつ $x^2 \equiv 1 \pmod{n}$ なる (x, n) が見つかったとき, n は素数ではない.

ミラー・ラビンテスト

ミラー・ラビンテスト (Miller-Rabin test):n は素数か?

- STEP1: n 未満の正の整数 a(証拠) を任意に取る.
- STEP2: $n-1=2^kq$ を満たす整数 k と奇数 q を求める.
- STEP3: $a^q \equiv \pm 1 \pmod{n}$ ならば n は素数である可能性が高いとして終了.
- STEP4: *i* = 1,···, *k* − 1 に対し STEP5, 6 を繰り返す.
- STEP5: a^{2^{iq}} ≡ -1 (mod n) ならば n は素数である可能性が高いとして終了.
- STEP6: $a^{2^{i_q}} \equiv 1$ ならば n は素数ではないとして終了.
- STEP7: n は素数ではないとして終了.

ミラー・ラビンテストの正当性

- n-1は偶数よりk≥0.
- $x \equiv \pm 1 \pmod{n} \Rightarrow x^2 \equiv \pm 1 \pmod{n}$ なので STEP3, 5 の条件 が満たされたとき $a^{2^kq} = a^{n-1} \equiv \pm 1 \pmod{n}$ が成立する.
- STEP6 は定理 A4 の対偶より従う.
- STEP5, 6 の繰り返しを抜けて STEP7 に到達したとき, $a^{2^kq} = a^{n-1} \not\equiv 1 \pmod{n}$ なので n は素数ではない.

ミラー・ラビンテストの性能

- O(log³n) らしい. ³
- ランダムな証拠 a に対し 75% 以上の確率で正しい結果を得 られる
- 100 個証拠を取ってくるとエラーの確率は 2²⁰⁰ 分の 1 未満に なる.
- n に対して高速に動くので $O(\sqrt{n})$ だと時間がかかる $n=10^{30}$ くらいの素数を判定させてみたいところだが、C++だと整数 型の最大値がボトルネックになり実験できない。
- C++の longlong 型で 9×10¹⁸ くらいだが, mod 累乗のところ で n^2 がオーバーフローしないことが条件となるので $n = 3 \times 10^9$ くらいまでしか判定させられない.

参考文献

- [1] http://www.compassare.org/fer-little.html
- [2] http://techtipshoge.blogspot.com/2014/04/blog-post_5.html
- [3] https://ja.wikipedia.org/wiki/ミラー-ラビン素数判定法

Chapter13-1:暗号学 Chapter13-2:素数判定 Chapter13-3:ミラー・ラビンテスト

● 後半へ続く.