Cryptography Final Report PRIMES is in P[1]

臺灣大學資訊工程學系 B04902012 劉瀚聲

在得知這學期的密碼學報告可以自選相關主題時，腦海中浮現的第一選擇，便是這篇「PRIMES is in P」。質數在大多數的密碼系統中，往往是相當重要的一環。一個有效率的質數判別算法對密碼學的貢獻不言自明。身爲一個資工系學生，目前的研究領域又是關於演算法與複雜度，這篇論文一直在我的 Wishing List 的前幾位。PRIMES 屬於 coNP 相當顯然，但 PRIMES 在 NP 內並不直觀。可以想像，這篇論文的在 2002 年的發表震驚了多少猜測 PRIMES 屬於 NP-Complete 或 coNP-Complete 的學者。

一些教授和網路上大多數的網友對這篇論文的評價都是「直白易懂」、「半小時內可以讀完」之類。但我親自讀之後，並不覺得它有傳聞中的那麼簡單。除了某些引理用到了一些我不曾學過的定義和性質（如分圓多項式等），相對影響較大的，是裡面某些推導或敘述並沒有給出詳細的原因，試著把敘述的正確性證明一次，卻發現原因並不顯然等諸如此類的情況。這些過程在這篇報告中會詳細的證明，而這樣的心得，會以腳註的方式寫在報告中。

爲了證明自己有學到東西，這篇報告是用中文寫成（再附上 LaTeX 原始碼），至少能表示有理解論文的內容而不是抄襲而得。此外，也把證明的架構系統化，改成自己比較喜歡的形式。我所讀過的論文，大多是 Top-down 的架構。在這篇報告中，定理會在後面的其他節證明，而引理會在當節的最後證明。如此一來，讀者在熟悉整個證明之前，便可以先了解證明的架構、知道每一個定理與引理在證明中的地位，之後再選擇想了解的定理與引理閱讀其證明。

在開始寫起這篇報告後，才發現貫徹這些原則有許多困難：用中文寫數學證明實在是太痛苦了。一來是習慣用用英文思考，翻成中文往往很奇怪，二來是論文中有一些作者自己創造的專有名詞（如”introspective”，意譯成自省函數很奇怪，但原封不動的將英文單字夾在中文報告中又顯得突兀。幾經思索，決定按照函數的特性，擅自翻譯成冪同態）等等，果然還是好想用英文寫啊。

正如我的專題指導教授所言，易寫則難讀，易讀則難寫。期許我的這篇報告費盡心思的結果，能讓所有想認識這個演算法的讀者快速了解其運作及正確性。

整個演算法以引理 2.1 爲核心。事實上，引理 2.1 已經提供了一個顯然充分的質數判別法：枚舉 $[0, n-1]$ 中的所有 a，並檢驗

$$(X+a)^n \equiv X^n + a \pmod n$$

是否成立，但這樣一來迭代的次數就高達 n 次，而且 n 次多項式的乘法與比較需要的時間也是 $O(n)$，但輸入規模是 $O(\lg n)$。在這個算法中，解決迭代次數過多的方法是將 a 的範圍縮減到 $[0, l]$，而解決多項式次數過高的方法是在模 $(X^r - 1)$ 的剩餘類環上進行運算和比較。但如此一來，這個算法作爲質數檢驗法的充分性就不再顯然，而 l 和 r 的上界也需要證明。

0 Notation

$\mathbb{Z}_r$ 表示整數模 r 形成的環，而 $\mathbb{Z}_r^*$ 表示與 r 互質的整數模 r 形成的乘法群。

$\mathbb{F}_p$ 表示 p 個元素的有限體，而 $f(X) \equiv g(X) \pmod{h(X), p}$ 表示在 $\mathbb{Z}_p[X]/(h(X))$ 上，$f(X) = g(X)$。[1]

$\phi(r)$ 表示小於 r 且與 r 互質的自然數個數，而對於 $(a, r) = 1$，$o_r(a)$ 表示在 $\mathbb{Z}_r^*$ 中 a 的週期。亦即，$o_r(a) = \min\{k | k \in \mathbb{N}, a^k \equiv 1 \pmod r\}$。顯然，$o_r(a) \mid \phi(r)$。

1 Algorithm and Proof Sketch

Algorithm 1.1 判定質數的算法

```
0 Input: integer n > 1.
1 If n = a^b for some a ∈ ℕ and b > 1, output COMPOSITE.
2 Find the smallest r such that o_r(n) > lg^2 n.
3 If 1 < (a,n) < n for some a ≤ r, output COMPOSITE.
4 If n ≤ r, output PRIME.
5 For a from 1 to ⌊sqrt(φ(r)) lg n⌋ do:
        If (X+a)^n ≢ X^n + a (mod X^r − 1, n), output COMPOSITE.
6 Output PRIME.
```

[1] 原論文中，作者強調 $h(X)$ 須爲不可約多項式，但論文中最常用到的是 $\pmod{X^r-1, p}$，而 (X^r-1) 並非不可約多項式。

Theorem 1.2 當算法 1.1 輸出 `COMPOSITE` 時，n 爲合數

第 2 節爲定理 1.2 之證明。

Theorem 1.3 當算法 1.1 輸出 `PRIME` 時，n 爲質數

第 3 節爲定理 1.3 之證明。

Theorem 1.4 算法 1.1 的時間複雜度爲 $O(\lg^{12} n)$

第 4 節爲定理 1.4 之證明。

定理 1.2 及定理 1.3 保證了算法的正確性。而由於輸入規模爲 $\lg n$，定理 1.4 保證了算法的運行時間爲多項式時間。故算法 1.1 是一個 PRIME 的多項式時間算法。[2]

2 Correctness When Output COMPOSITE

當算法在第 1 步或第 3 步輸出 COMPOSITE 時，n 是合數，因爲第 1 步的 a 和第 3 步的 (a, n) 會是一個 n 的非平凡因數。

Lemma 2.1 $a \in \mathbb{Z}$，$n \in \mathbb{N}$，$n \geq 2$，$(a, n) = 1$，那麼 n 爲質數若且唯若

$$(X + a)^n \equiv X^n + a \pmod{n}$$

當算法在第 5 步輸出 COMPOSITE 時，表示 $(X + a)^n \not\equiv X^n + a \pmod{X^r - 1, n}$，因此 $(X + a)^n \not\equiv X^n + a \pmod{n}$。根據引理 2.1，$n$ 爲合數。

2.1 Proof to Lemma 2.1

根據二項式定理，$\forall 0 < i < n$，$(X + a)^n$ 中 X^i 的係數爲 $C_i^n a^{n-i}$，而 X^n 的係數顯然同餘。

(1) n 爲質數

[2] 將演算法的 $\phi(r)$ 改爲 r 看起來並無不妥。

由於 $\forall 0 < i < n$，$C_i^n = \dfrac{n!}{i!(n-i)!}$，$n \mid (n!)$，$n \nmid (i!(n-i)!)$，故 $C_i^n a^{n-i} \equiv 0 \pmod{n}$。根據費瑪小定理，$a^n \equiv a \pmod{n}$。故 $(X+a)^n \equiv X^n + a \pmod{n}$。

(2) n 爲合數

對於 n 的任何一個質因數 q，若 $q^k \mid n$ 但 $q^{k+1} \nmid n$，那麼由於 $C_q^n = \dfrac{n(n-1)...(n-q+1)}{q(q-1)(q-2)...(1)}$，而 $q^k \nmid \dfrac{n}{q}$，且分子及分母中之其他項皆與 q 互質，故 $n \nmid C_q^n$。亦即，$C_q^n a^{n-q} \not\equiv 0 \pmod{n}$。

綜合以上兩種情況，引理得證。

3 Correctness When Output PRIME

當算法在第 4 步輸出 PRIME 時，n 爲質數。因爲第 3 步和 $n \le r$ 保證了 $\forall a < n$，$(a,n) = 1$。以下證明算法在第 6 步輸出 PRIME 的正確性。

由於 $o_r(n) > 1$，n 必定有質因數 p 滿足 $o_r(p) > 1$。又因爲通過了第 3 步和第 4 步的檢驗，所以 $(r,n) = 1$，且 $p > r$，故 $p, n \in \mathbb{Z}_r^*$。另外，令 $l = \lfloor \sqrt{\phi(r)} \lg n \rfloor$。在第 5 步中，算法檢驗了 l 個等式。由於第 5 步沒有輸出 COMPOSITE，因此對於所有的 $0 \le a \le l$，都有：

$$(X+a)^n \equiv X^n + a \pmod{X^r - 1, n}$$

由於 p 是 n 的因數，故：

$$(X+a)^n \equiv X^n + a \pmod{X^r - 1, p}$$

由於 p 是質數，故：

$$(X+a)^p \equiv X^p + a \pmod{X^r - 1, p}$$

Lemma 3.1 $(X+a)^{\frac{n}{p}} \equiv X^{\frac{n}{p}} + a \pmod{X^r - 1, p}$。

對於多項式函數 f 和自然數 m，定義 m 對於 f 是冪同態的，表示 $f(X)^m \equiv f(X^m) \pmod{X^r - 1, p}$。由上面的敘述可知，對所有的 $0 \le a \le l$，n、p、$\dfrac{n}{p}$ 對於 $(X+a)$ 都是冪同態的。

Lemma 3.2 如果 m_1、m_2 對於 $f(X)$ 都是冪同態的，那麼 m_1m_2 對於 $f(X)$ 也是冪同態的。

Lemma 3.3 如果 m 對於 $f_1(X)$、$f_2(X)$ 都是冪同態的，那麼 m 對於 $f_1(X)f_2(X)$ 也是冪同態的。

接下來考慮以下幾個集合：令 $I = \{p^i(\frac{n}{p})^j | i, j \geq 0\}$，$P = \{\prod_{a=0}^{l}(X+a)^{e_a} | e_a \geq 0\}$。根據引理 3.2 和 3.3，$I$ 中的每一個元素對於 P 中的每一個元素都是冪同態的。

由於 n、p、$\frac{n}{p}$ 都分別和 r 互質，故 I 模 r 所形成的集合會在 $\mathbb{Z}_r^*$ 內，而且是一個乘法群。令 G 爲那個群，亦即，$G = I/r\mathbb{Z} = \{p^i(\frac{n}{p})^j \mod r | i, j \geq 0\}$，並令 $t = |G|$。

由於 $o_r(n) > \lg^2 n$，故 $t > \lg^2 n$。令 $Q_r(X)$ 爲 r 次分圓多項式，根據分圓多項式的性質，$Q_r(X) \mid (X^r - 1)$，且在 $\mathbb{F}_p$ 上，$Q_r(X)$ 是若干個 $o_r(p)$ 次不可約多項式的乘積。令 $h(X)$ 是其中一個這樣的多項式。由於 $o_r(p) > 1$，故 $\deg(h(X)) > 1$。令 $F = \mathbb{F}_p[X]/(h(X))$，而 $\mathcal{G}$ 爲 P 模 $h(X)$ 再把係數模 p 得到的集合。由於 $h(X)$ 不可約，故 F 和 $\mathcal{G}$ 都是乘法群。

可以觀察到 G 爲 $\mathbb{Z}_r^*$ 的乘法子群，而 $\mathcal{G}$ 爲 F 的乘法子群。故 $t \leq \phi(r)$。

Lemma 3.4 $|\mathcal{G}| \geq \binom{t+l}{t-1}$。

Lemma 3.5 若 n 不是 p 的冪次，則 $|\mathcal{G}| \leq n^{\sqrt{t}}$。

Lemma 3.6 對於 $k > 1$，$\binom{2k+1}{k} > 2^k$。

根據引理 3.4，

$$
\begin{aligned}
|\mathcal{G}| &\geq \binom{t+l}{t-1} \\
&\geq \binom{l+1+\lfloor\sqrt{t}\lg n\rfloor}{\lfloor\sqrt{t}\lg n\rfloor} (\because t \geq \lg^2 n) \\
&\geq \binom{2\lfloor\sqrt{t}\lg n\rfloor+1}{\lfloor\sqrt{t}\lg n\rfloor} (\because l = \lfloor\sqrt{\phi(r)}\lg n\rfloor \geq \lfloor\sqrt{t}\lg n\rfloor) \\
&> 2^{\lfloor\sqrt{t}\lg n\rfloor+1} (\because \sqrt{t}\lg n > 1) \\
&\geq n^{\sqrt{t}}
\end{aligned}
$$

故根據引理 3.5，n 爲 p 的冪次。但由於第 1 步沒有輸出 COMPOSITE，故 $n = p$，即 n 是個質數，定理得證。

3.1 Proof to lemma 3.1[3]

$$
\begin{aligned}
(X^{\frac{n}{p}} + a)^p &\equiv X^n + a \\
&\equiv ((X+a)^{\frac{n}{p}})^p \pmod{X^r - 1, p}
\end{aligned}
$$

故只須證明對於多項式 $f(X)$、$g(X) \in \mathbb{Z}_p[X]/(X^r - 1)$，$f^p(X) \equiv g^p(X) \pmod{X^r-1, p} \Rightarrow f(X) \equiv g(X) \pmod{X^r-1, p}$。

但 $f^p(X) - g^p(X) \equiv 0 \pmod{X^r-1, p} \Rightarrow (f(X) - g(X))^p \equiv 0 \pmod{X^r-1, p}$（證明類似定理 2.1 的證明，展開後觀察係數）。故進一步，只須證明

$(f(X) - g(X))^p \equiv 0 \pmod{X^r-1, p} \Rightarrow (f(X) - g(X)) \equiv 0 \pmod{X^r-1, p}$。

其充分條件是對於多項式 $z(X) \in \mathbb{Z}_p[X]/(X^r - 1)$，

$z^p(X) \equiv 0 \pmod{X^r-1, p} \Rightarrow z(X) \equiv 0 \pmod{X^r-1, p}$。

假設 $z^p(X) \equiv 0 \pmod{X^r-1, p}$，那麼存在多項式 $q(X)$ 使得 $z^p(X) \equiv q(X)(X^r-1) \pmod{p}$。

若 $(X^r - 1) \nmid z(X)$，那麼 $(X^r - 1)$ 必有重數大於 1 的因式。亦即存在多項式 $q_1(X)$、$q_2(X)$ 滿足 $(X^r - 1) \equiv [q_1(X)]^2 q_2(X) \pmod{p}$，且 $\deg(q_1(X)) > 1$。但考慮 $(X^r - 1)$ 之形式微分：

[3]原論文對本引理的證明隻字未提，彷彿這個引理的結論十分直觀。若 F 爲體，那麼由於沒有零因子，故引理顯然成立，但 $(X^r - 1)$ 可約。

$$(X^r-1)' \equiv rX^{r-1} \pmod p，$$
$$([q_1(X)]^2 q_2(X))' \equiv 2q_1(X)q_1'(X)q_2(X) + [q_1(X)^2 q_2'(X) \pmod p。$$

但 $(X^r-1,(X^r-1)') \equiv 1 \pmod p$，$q_1(X) \mid ([q_1(X)]^2 q_2(X), ([q_1(X)]^2 q_2(X))')$，矛盾，故 $(X^r-1) \mid z(X)$，即引理得證。

3.2 Proof to lemma 3.2

$[f(X)]^{m_1 m_2} \equiv [f(X^{m_1})]^{m_2} \pmod{X^r-1, p}$

$[f(X^{m_1})]^{m_2} \equiv f(X^{m_1 m_2}) \pmod{X^{rm_1}-1, p}$

由於 $(X^r-1) \mid (X^{rm_1}-1)$，故
$[f(X)]^{m_1 m_2} \equiv f(X^{m_1 m_2}) \pmod{X^r-1, p}$，
引理得證。

3.3 Proof to lemma 3.3

$[f_1(X)^m \equiv f_1(X^m) \pmod{X^r-1, p}$，

$[f_2(X)^m \equiv f_2(X^m) \pmod{X^r-1, p}$，

故 $[f_1(X)f_2(X)]^m \equiv f_1(X^m)f_2(X^m) \pmod{X^r-1, p}$，引理得證。

3.4 Proof to lemma 3.4

由於 $h(X) \mid Q_r(X)$，根據分圓多項式的性質，r 爲最小的自然數滿足在 F 上 $X^r = 1$。

以下證明 P 中任兩個相異的、低於 t 次的多項式，在 F 上也相異。

令 $f(X)$ 和 $g(X)$ 就是兩個這樣的多項式，亦即，$f(X)$、$g(X) \in P$，$f(X) \neq g(X)$，$\max(\deg(f(X)), \deg(g(X))) < t$。假設在 F 上，$f(X) = g(X)$。

令 $m \in I$，顯然在 F 上 $[f(X)]^m = [g(X)]^m$。由於 m 對於 $f(X)$ 和 $g(X)$ 都是冪同構的，而且 $h(X) \mid (X^r-1)$，故在 F 上，$f(X^m) = g(X^m)$。這表示對所有的 $m \in G$，(X^m) 都是 $f(Y) - g(Y) = 0$ 的一個根。以下證明這 $|G| = t$ 個根全部相異。

假設有相異的 m_1、$m_2 \in G$，滿足在 F 上 $X^{m_1} = X^{m_2}$。不失一般性假設

$m_1 > m_2$，那麼 $X^{m_1-m_2} = 1$。但注意到由於 G 爲 $\mathbb{Z}_r^*$ 的子群，導致 $(m_1 - m_2) < r$，這與證明開頭提到的 r 的最小性矛盾。故那 t 個根全部相異。

但 $\deg(f(Y) - g(Y)) < t$，與他有 t 個相異根矛盾，故 P 中任兩個相異的、低於 t 次的多項式，在 F 上也相異。

P 中低於 t 次多項式的個數，與方程 $\sum_{a=0}^{l} e_a \le t-1$ 的非負整數解的個數相同。令 $d = (t-1) - \sum_{a=0}^{l} e_a$，那麼該方程解的個數又與 $\sum_{a=0}^{l} e_a + d = t-1$ 的非負整數解的個數相同，爲 $H_{t-1}^{l+2} = \binom{t+l}{t-1}$。由於這 $\binom{t+l}{t-1}$ 在 F 上也全部相異，故 $\mathcal{G}$ 中也至少有 $\binom{t+l}{t-1}$ 個相異元素。引理得證。

3.5 Proof to lemma 3.5

考慮 I 的子集 $\hat{I} = \{p^i(\frac{n}{p})^j | i,j \le \lfloor\sqrt{t}\rfloor\}$。

若 n 不是 p 的冪次，那麼 $\hat{I}$ 中的元素全部相異，$|\hat{I}| = (\lfloor\sqrt{t}\rfloor + 1)^2 > t$。由於 $|G| = t < |\hat{I}|$，故 $\hat{I}$ 中必定有相異元素 m_1 和 m_2 模 r 同餘。不失一般性，假設 $m_1 > m_2$。那麼，

$$X^{m_1} \equiv X^{m_2} \pmod{X^r - 1}。$$

令 $f(X) \in P$。

$$\begin{aligned} [f(X)]^{m_1} &\equiv f(X^{m_1}) \\ &\equiv f(X^{m_2}) \\ &\equiv [f(X)]^{m_2} \end{aligned}$$

亦即，在 F 上，$[f(X)]^{m_1} = [f(X)]^{m_2}$，故在 F 上，對於所有的 $f(X) \in \mathcal{G}$，$f(X)$ 都是 $Y^{m_1} - Y^{m_2} = 0$ 的根。但注意到 $\deg(Y^{m_1} - Y^{m_2}) = m_1 \le (\frac{n}{p} \times p)^{\lfloor\sqrt{t}\rfloor} \le n^{\sqrt{t}}$，最多只有 $n^{\sqrt{t}}$ 個根，故 $|\mathcal{G}| \le n^{\sqrt{t}}$。引理得證。

3.6 Proof to lemma 3.6[4]

使用數學歸納法。

當 $k = 2$ 時，$\binom{2\times2+1}{2} = 10 > 2^{2+1}$，敘述成立。

[4]也是一個在原論文中被直接使用的結論，這邊給出證明。

假設當 $k=k_0-1$ 時，$\binom{2k_0-1}{k_0-1} > 2^{k_0}$，

那麼當 $k=k_0$ 時，$\binom{2k_0+1}{k_0} = \binom{2k_0}{k_0} + \binom{2k_0}{k_0-1}$，

其中 $\binom{2k_0}{k_0} = (\frac{2k_0}{k_0})(\frac{2k_0-1}{k_0-1})...(\frac{k_0+1}{1}) \geq (2)(2)...(2) = 2^{k_0}$，

而 $\binom{2k_0}{k_0-1} > \binom{2k_0-1}{k_0-1} > 2^{k_0}$。

故 $\binom{2k_0+1}{k_0} > 2^{k_0}+2^{k_0} = 2^{k_0+1}$，敘述亦成立。

從而，根據數學歸納法，引理得證。

4 Time Complexity of Algorithm

第 1 步枚舉 b 自 1 至 $\lg n$，二分搜尋對應的 a，檢驗 a^b 與 n 的關係。時間複雜度 $O(\lg^3 n)$。

第 2 步自 1 開始枚舉 r，檢驗是否 $\forall 1 \leq i \leq \lg^2 n$，$n^i \not\equiv 1 \pmod r$。時間複雜度 $O(r \lg^3 n)$。

第 3 步枚舉 a 自 1 至 r，計算 (a,n)。時間複雜度 $O(r \lg n)$。

第 4 步時間複雜度 $O(1)$。

第 5 步每次迭代可用快速冪在 $\lg n$ 次多項式乘法內算出 $(X+a)^n \pmod{X^r-1, n}$ 的值，而多項式的次數不超過 r，故時間複雜度爲 $O((\sqrt{\phi(r)}\lg n)(r^2 \lg n)) = O(r^{\frac{5}{2}} \lg^2 n)$。

第 6 步時間複雜度 $O(1)$。[5]

故整體時間瓶頸爲第 5 步，複雜度爲 $O(r^{\frac{5}{2}} \lg^2 n)$。故只須證明 r 的上界。

令 $B = \lceil \lg^5 n \rceil$，$S = n^{\lfloor \lg B \rfloor} \prod_{i=1}^{\lfloor \lg^2 n \rfloor} (n^i - 1)$。[6]

$S < n^{\lfloor \lg B \rfloor} \prod_{i=1}^{\lfloor \lg^2 n \rfloor} (n^i) = n^{\lfloor \lg B \rfloor + \frac{1}{2} \lg^2 n (\lg^2 n - 1)} \leq n^{\lg^4 n} \leq 2^B$。

考慮 $R = \min\{R' | R' \nmid S\}$，由於 $\forall i \in [1, \lfloor \lg^2 n \rfloor], R \nmid (n^i - 1)$，故 $o_R(n) > \lg^2 n$，亦即 R 是 r 的一個上界。

[5]原論文在分析時間複雜度時，將整數乘法的時間複雜度算爲 $\Theta(n)$，這邊按照習慣，算爲常數時間。
[6]將 $n^{\lfloor \lg B \rfloor}$ 刪除看起來並無不妥，在後續的證明並沒有用到。

Lemma 4.1 *(Nair)*[2] 令 $LCM(m)$ 表示前 m 個自然數的最小公倍數，那麼對於 $m \geq 7$，$LCM(m) \geq 2^m$。

假設 $R > B$，那麼 $\forall i \leq B$，$i \mid S$，亦即 $S \mid LCM(B)$，但根據引理 4.1，$LCM(B) \geq 2^B > S$，矛盾，故 $R \leq B$。從而，$r \leq \lg^5 n$，定理得證。[7]

5 References

[1] M. Agrawai, N. Kayal, N. Saxena. *Annals of Math.* 781-793, 2004.

[2] M. Nair. On Chebyshev-type inequalities for primes. *Amer. Math. Monthly* 89:126 129, 1982.

[7]原論文在這之前亦證明了 $(n, R) = 1$，但這應該是算法的第 3 步所保證的。