MỞ RỘNG LỚP CÁC SỐ MERSENNE

Lều Đức Tân

Ban cơ yếu chính phủ

Mở đầu

Năm 1640 Mersenne xét lớp các số có dạng $M_n = 2^n - 1$ và đề ra giả thuyết rằng: với $n < 257$ thì M_n là nguyên tố khi và chỉ khi $n = 2, 3, 5, 7, 31, 67, 127$ và 257.

Guồng máy xác định nhận định trên và hơn nữa để khảo sát một lớp các số có dạng $M_n = 2^n - 1$ với n nguyên tố bắt đầu hoạt động. Các số M_2, M_3, M_5 và M_7 đã được biết là nguyên tố từ thời Euclide. M_{13} cũng được biết từ 1461 nhưng không xác định rõ tác giả. Năm 1732, Euler đã chỉ ra M_{29} là hợp số và năm 1750 chỉ ra M_{31} là nguyên tố. Nhận định của Mersenne đứng vững hơn 200 năm cho đến khi Lucas chỉ ra rằng M_{67} là hợp số vào năm 1876. Cho đến 1914 giả định của Mersenne mới được bổ xung thêm. Ông đã sai trong 5 trường hợp: Thiếu M_{61} (do I.M. Pervushin chỉ ra 1883), M_{89} M_{107} (do R.E. Powers và E. Fauquenberg chỉ ra 1914). Và thừa M_{67}, M_{257}.

Trong quá trình giải bài toán trên của Mersenne đã hình thành lên một loại kiểm tra tính nguyên tố cho các số nguyên và được gọi là thuật toán kiểm tra tính nguyên tố kiểu-$(N+1)$ như sau:

> *Giả sử ta biết được khai triển $N+1$ thành tích các thừa số nguyên tố và D là một số sao cho $J(D/N) = -1$. Nếu với mỗi ước nguyên tố p của $N+1$, có một dãy Lucas U_k với biệt thức D sao cho N là ước của U_{N+1} nhưng không là ước của $U_{(N+1)/p}$ thì N là nguyên tố.*

Trong phát biểu trên, $J(D/n)$ là ký hiệu Jacobi, còn khái niệm dãy *Lucas* được định nghĩa ở phần 0. Kết quả tốt nhất về loại thuật toán này cho bởi định lý sau

Định lý Lucas. *Cho $N = R2^k - 1$ với R lẻ $< 2^k$ và 3 không là ước của R và N. Khi đó N nguyên tố khi và chỉ khi $V_{(N+1)/4} \equiv 0 \ mod \ N$.*

Với kết quả trên không những kiểm tra tính nguyên tố cho các số thuộc lớp các số Mersenne mà còn kiểm tra được cho một số lớp rộng hơn nhiều. Trong bài này chúng tôi sẽ mở rộng hơn nữa tầm hiệu lực của thuật toán kiểu $N+1$ nói trên.

Bài báo này nhằm giải quyết vấn đề xây dựng cơ sở lý thuyết cho một thuật toán kiểm tra tính nguyên tố kiểu $N+1$ và từ đó tìm kiếm nhanh các số nguyên tố lớn trong một lớp số được ký hiệu là lớp LM.

Ta có thể xuất phát từ định lý sau đây.

Định lý Lehmer ([17]). *Cho $N = RF - 1$, $(F, R) = 1$. Nếu $\{U_m\}$ là dãy Lucas với $J(D/N) = -1$ sao cho với mọi ước nguyên tố q của F ta có $U_{N+1} \equiv 0 \ mod \ N$ và $(U_{(N+1)/2}, N) = 1$ thì mọi ước nguyên tố p của N đều có dạng $p = mF \pm 1$.*

Tuy nhiên việc chỉ ra dãy Lucas thoả mãn điều kiện của định lý không phải dễ dàng, do vậy kết quả khả quan nhất có tính thực hành liên quan đến thuật toán kiểu $N+1$ chỉ đạt đến kết quả của Lucas đã nêu ở trên. Chúng tôi đã tìm ra một kết quả (định lý 3) tương tự nhưng yếu hơn kết luận của Lehmer nhưng để bù lại chúng tôi đã chỉ ra có tính kiến thiết (điều kiện 7) lớp số cụ thể (lớp LM) mà trên đó việc viết chương trình kiểm tra tính nguyên tố các số thuộc lớp đó lại hết sức đơn giản. Ngoài ra chúng tôi đã chứng tỏ được việc tham gia của tham số d trong bước kiểm tra tính nguyên tố kiểu $N+1$ vẫn còn có hiệu lực (định lý 4) do vậy đã xây dựng được thuật toán NT mà lớp các số kiểm tra được của nó lớn hơn hẳn lớp các số kiểm tra được của thuật toán của Lucas về bậc.

Nội dung của báo gồm các phần sau:

Phần 0 nhằm giới thiệu về khái niệm dãy Lucas và các kết quả liên quan đến việc chứng minh các kết quả ở các phần sau.

Trong phần 1 chúng tôi chứng minh thêm một số tính chất khác cần cho mục đích về sau.

Phần 2 bao gồm các kết quả chính để xây dựng một lớp số và một thuật toán đa thức để kiểm tra tính nguyên tố đối với các số thuộc lớp đó.

Trong phần 3 chúng tôi đưa ra kết quả tính toán thu được khi thực hiện tìm kiếm các nguyên tố bằng thuật toán xây dựng được ở phần trên.

0. Các khái niệm và kết quả liên quan

0.1. *Ký hiệu Legendre và ký hiệu Jacobi*

Cho p nguyên tố và a là số nguyên tố đối với p, khi đó số

$$L(a/p) = \begin{cases} 1, & \text{nếu có } b \text{ sao cho } a \equiv b^2 \ mod \ p \\ -1, & \text{trong trường hợp ngược lại} \end{cases}$$

được gọi là ký hiệu Legendre của a và p.

Định nghĩa 0.2. Cho m, n nguyên với $n > 3$, $(m,n) = 1$. Nếu $n = p_1p_2...p_r$ trong đó p_i là các nguyên tố (không nhất thiết khác nhau) ta gọi $J(m/n) = L(m/p_1)L(m/p_2)...L(m/p_r)$ là ký hiệu Jacobi của m và n.

Định lý 0.3 (luật bình phương tương hỗ). *Cho các số nguyên lẻ m,n với $(m,n) = 1$, khi đó*

$$J(m/n) = (-1)^{1/4(M-1)(N-1)}J(n/m).$$

Định lý 0.4. *Nếu p là nguyên tố lẻ khi đó với mọi a mà $(a,p) = 1$ ta có $J(a/b) = L(a/p) = a \bmod p$.*

Các kết quả trên có thể tìm trong [1].

Các kết quả trên trường $Z_p(\sqrt{D})$

Cho p nguyên tố khi đó vành dồng du modulo p, ký hiệu là Z_p, là trường hữu hạn p phần tử. Nếu d là số sao cho p không là ước cuả D ta ký hiệu

$$Z_p(\sqrt{D}) = \{x + y\sqrt{D} |\ x,y \in Z_p\}$$

và xây dựng các phép toán trên đó như sau:

Nếu $a_1 = x_1 + y_1\sqrt{D}$ và $a_2 = x_2 + y_2\sqrt{D}$ ta gọi tổng a_1 và a_2 là phần tử ký hiệu $a_1 + a_2$ xác định bởi công thức

$$a_1 + a_2 = (x_1 + x_2)(y_1 + y_2)\sqrt{D}.$$

và tích của a_1 và a_2 là phần tử ký hiệu là $a_1.a_2 = (x_1x_2 + y_1y_2D) + (x_1y_2 + x_2y_1)\sqrt{D}$

Kết quả 0.5. Tập $Z_p(\sqrt{D})$ với các phép toán cộng và nhân xây dựng ở trên là trường. Hơn nữa nếu $J(D/p) = 1$ thì $Z_p(\sqrt{D}) \equiv Z_p$ còn nếu $J(D/p) = -1$ thì $Z_p(\sqrt{D})$ là trường mở rộng cuả Z_p với số phần tử là p.

Định lý 0.6. (Định lý Fermat trên $Z_p(\sqrt{D})$. *Với $a \neq 0$ và $a \in Z_p(\sqrt{D})$ ta có*

$$(a)\ a^{p-1} \equiv 1 \bmod p \text{ khi } (D/p) = 1,$$

$$(b)\ a^p \equiv a^* \bmod \text{khi } (D/p) = -1$$

ở đây $a^* = x - y\sqrt{D}$ (với $a = x + y\sqrt{D}$) và gọi là liên hợp cuả a.

Các kết quả trên có thể tìm trong [15] hay [17].

0.3. *Dãy Lucas*

Cho phương trình với hệ số P, Q nguyên

$$\lambda^2 - P\lambda + Q = 0. \tag{1}$$

Giả sử a và b là hai nghiệm của phương trình (1) với $m \geq 0$ ta ký hiệu

$$U_m = (a^m - b^m)/(a-b) \text{ và } V_m = a^m + b^m. \tag{2}$$

Định nghĩa 0.7. Dãy các số $\{U_m\}$, $\{V_m\}$ gọi là dãy Lucas của phương trình (1) và phương trình (1) gọi là phương trình đặc trưng của dãy Lucas $\{U_m\}$, $\{V_m\}$ với U_m, V_m xác định ở công thức (2).

Ta thấy rằng $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$ là các số nguyên.

Công thức 0.8. Với $m \geq n \geq 0$ ta có

$$\begin{cases} U_{m+n} = U_m V_n - Q^n U_{m-n} \\ V_{m+n} = V_m V_n - Q^n V_{m-n}. \end{cases} \tag{3}$$

Trường hợp $n = 1$

$$\begin{cases} U_{m+n} = PU_m - QU_{m-1} \\ V_{m+n} = PV_m - Q^n V_{m-1}. \end{cases} \tag{4}$$

Trường hợp $m = n$

$$\begin{cases} U_{2mn} = U_m V_m \\ V_{2m} = V_{2m} - 2Q^m. \end{cases} \tag{5}$$

Trường hợp $m = n + 1$.

$$\begin{cases} U_{2m-1} = U_m V_{m-1} - Q^{m-1} \\ V_{2m-1} = V_m V_{m-1} - PQ^{m-1}. \end{cases} \tag{6}$$

Tính chất 0.9. *Cho dãy Lucas $\{U_m\}$ khi đó nếu i là ước của j thì U_i là ước của U_j.*

Tính chất 0.10. *Với mọi $M \geq 0$ ta có*

$$\begin{bmatrix} U_{m+1} & V_{m+1} \\ U_m & V_m \end{bmatrix} = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix}^m \begin{bmatrix} U_1 & V_1 \\ U_0 & V0 \end{bmatrix}.$$

Tính chất 0.11. *Cho $\{U_m\}$ là dãy Lucas của phương trình $\lambda^2 - P\lambda + Q = 0$ với biệt thức $P^2 - 4Q = x^2 D$ trong đó D không có thừa số chính phương. Khi đó nếu số nguyên tố p không là ước của $D.Q$ thì $U_{p-J(D/p)} \equiv 0 \ mod\ p$.*

Điều kiện Riesel 0.12. *Phương trình đặc trưng $\lambda^2 - P\lambda + 1 = 0$ với biệt thức $P^2 - 4 = x^2 D$ trong đó $J(D/N) = -1$ và D không có thừa số chính phương, có nghiệm $a = b^2/r$ sao cho*

$$bb^*/r) J(r/N) = -1, \tag{7}$$

ở đây b^* là liên hợp của b được gọi là thoả mãn điều kiện Riesel đối với N.

Định lý 0.13 (xem [17]) *Cho $N = R2^{k-1} - 1$ với R lẻ $R \leq 2^k$ và $\{V_m\}$ là dãy Lucas của phương trình thoả mãn điều kiện Riesel đối với N. Khi đó 2 điều kiện sau là tương đương:*

(a) N nguyên tố

(b) $V_{(N+1)/4} \equiv 0 \mod N$.

1. Các kết quả lý thuyết

1.1. *Bổ xung về tính chất của dãy Lucas*

Từ tính chất 0.11 ta có quyền định nghiã như sau:

Định nghiã 1.1. Ta gọi giá trị $d = \min_{m>0}\{U_m \equiv 0 \mod p\}$ với p nguyên tố không là ước của D. Q là bậc của $\{U_m\}$ đối với p, ở đây $\{U_m\}$ là dãy Lucas của phương trình đặc trưng $\lambda^2 - P\lambda + Q$.

Ta có tính chất sau đây.

Tính chất 1.2. *Nếu d là bậc của $\{U_m\}$ đối với p và nếu $U_m \equiv 0 \mod p$ thì d là ước của m.*

Chứng minh. Giả sử

$$m = qd + r \text{ với } 0 \leq r \leq d. \tag{8}$$

Trường hợp $q = 2t - 1$ (tr. 1)

$$\begin{aligned} U_m &= U_{td+((t-1)d+r} \\ &= U_{td}V_{(t-1)d+r} - Q^{(t-1)d+r}U_{d-r}. \end{aligned} \tag{9}$$

Từ định nghiã 1 ta có p là ước của U_d mà d là ước của td nên theo tính chất 0.9 ta có U_d là ước của U_{td} nên p là ước của U_{td} mặt khác p là ước của

$$U_m = = U_{td}V_{(t-1)d+r} - Q^{(t-1)d+r}U_{d-r},$$

do đó ta có p là ước của $Q^{(t-1)d+r}U_{d-r}$ mà p không là ước của Q vậy p là ước của U_{d-r}.

Do d là bé nhất nên $d \leq d - r$ hay $r = 0$.

Trường hợp $q = 2t$

Rõ ràng ta chỉ cần xét với $t \geq 1$ và như vậy $m = qd + r = 2td + r = (t+1)d + (t-1)d + r$ nên $U_m = U_{(t+1)d+(t-1)d+r}$ theo công thức 0.8 [3] thì

$$U_{(t+1)d+(t-1)d+r} = U_{(t+1)d}V_{(t-1)d+r} - Q^{(t-1)d+r}U_{2d+r}.$$

Lập luận như trường hợp trên ta có $U_{2d-r} \equiv \mod p$. Như vậy lại từ công thức 0.8 [3] ta có

$$0 \mod p \equiv U_{2d-r} = U_{d+d-r} = U_dV_{d-r} - Q^{d-r}U_r$$

cho nên $U_r \equiv 0 \mod p$ mà d bé nhất và theo [8] thì $r < d$ cho nên $r = 0$. Tóm lại ta đều có $m = qd$ hay d là ước của m.

1.2. *Kết quả chính*

Định lý 1.3. *Cho $N = R.2^k - 1$ với R lẻ. Cho $\{V_m\}$ là dãy Lucas của phương trình đặc trưng*

$$\lambda^2 - P\lambda + 1 = 0 \tag{10}$$

thoả mãn điều kiện Riesel đối với N. Khi đó ta có

(a) Nếu N nguyên tố thì $V_{(N+1)/4} \equiv 0 \mod N$.

(b) Nếu $V_{(N+1)/4} \equiv 0 \mod N$ thì mọi ước nguyên tố p của N đều có dạng $p = s2^{k-1} \pm 1$.

Chứng minh. Trước hết do hệ số Q của phương trình đặc trưng bằng 1 nên ta có tích hai nghiệm của phương trình (10) bằng 1 vậy nếu a là nghiệm của phương trình (10) thì a^* cũng là nghiệm và do đó bằng liên hợp của a.

Chứng minh (a)

$$\begin{aligned} V_{(N+1)/4} &= a^{(N+1)/4} + a^{-(N+1)/4} \\ &= a^{-(N+1)/4}(a^{(N+1)/2} + 1) \text{ mà } a = b^2/r \text{ nên} \\ &= a^{-(N+1)/4}(b^{N+1})/r^{(N-1)/2} + 1) \\ &= a^{-(N+1)/4}(bb^N)r/r^{(N-1)/2} + 1), \end{aligned}$$

do N nguyên tố theo các định lý 0.6 ta có $b^N \equiv b^* \mod N$ (với b^* là liên hợp của b) và theo định lý 0.4 ta có $r^{(N-1)/2} \equiv J(r/N) \mod N$ vậy

$$V_{(N+1)/4} = a^{-(N+1)/4}(bb^*/rJ(r/N) + 1)$$

từ điều kiện Riesel ta có $bb^*/rr^{(N-1)/2} = -1$ nên $bb^*/rr^{(N-1)/2} + 1 = 0$ hay $V_{(N+1)/4} \equiv 0 \mod N$.

Chứng minh (b)

Từ $V_{(N+1)/4} \equiv 0 \mod N$ theo lập luận trên ta có

$$bb^*/rr^{(N-1)/2} = -1 \mod N. \tag{11}$$

Mặt khác theo công thức 0.8 [5] ta có

$$U_{(N+1)/2} = U_{(N+1)/4}V_{(N+1)/4} \equiv 0 \mod N \tag{12}$$

Theo định nghĩa của dãy Lucas ta có

$$U_{(N+1)/4} = (a^{(N+1)/4} - a^{-(N+1)/4})/(a - a^{-1}).$$

Lập luận như phần trên thì

$$U_{(N+1)/4} = a^{-(N+1)/4}(bb^*/rr^{(N-1)/2} - 1)/(a - a^{-1}) \equiv (a^{(N+1)/4} - a^{-(N+1)/4})/(a - a^{-1}) \mod N,$$

từ N lẻ nên $(-2, N) = 1$ còn $a^{(N+1)/4}$ và $a - a^{-1}$ là các phần tử có ngược trong $Z_N(\sqrt{D})$ nên ta có

$$U_{(N+1)/4} \not\equiv 0 \text{ modulo } N. \tag{13}$$

Nếu p là ước nguyên tố cuả N thì từ các hệ thức (12) và (13) ta có

$$U_{(N+1)/2} \equiv 0 \bmod 9 \tag{14}$$

$$U_{(N+1)/4} \not\equiv 0 \text{ modulo } p. \tag{15}$$

Như vậy nếu d là bậc cuả U_m đối với p từ (14) và $(N+1)/4 = R2^{k-2}$ vậy 2^{k-1} là ước cuả d. Lại theo định lý 0.11 ta có $U_{p-L(D/p)} \equiv 0 \bmod p$ theo tính chất 2 thì d là ước cuả $p - L(D/p)$ do đó 2^{k-1} cũng là ước cuả $p - L(D/P)$ và ta có ngay

$$p = s2^{k-1} + L(D/p) = s2^{k-1} \pm 1.$$

1.3. *Các thừa số dạng $M2^k \pm 1$*

Định lý 1.3 đã cho chúng ta nhiều hơn một điều kiện cần cho một số là nguyên tố. Để đạt được thuật toán cần thiết chúng ta chứng minh định lý sau đây

Định lý 1.4. *Cho $N = Aq^2 + Bq - 1$ với q chẵn, $0 < B < q$, $A > 1$. Khi đó các điều kiện sau là tương đương:*

(a)

$$N = (xq + 1)(yq - 1) \text{ với } x,\ y \geq 1 \tag{16}$$

(b) tồn tại d thoả mãm $d_1 \leq d \leq d_2$ với $d_1 = (-B - A + 1)div(q - 1)$ còn $d_0 = 0$ nếu $A - B - 1 < 0$ và bằng $(A - B - 1)div(q+1)$ nếu $A - B - 1 \geq 0$ [17] sao cho $(B+dq)^2+4(A-d)$ chính phương [18].

Chứng minh. (a) $\Longrightarrow$ (b). Từ $N = (xq + 1)(uq - 1) = xyq^2 + (y - x)q - 1$ ta có $B = (y - x)\bmod q$ và $A = xy + (y - x)\text{div } q$. Đặt $d = (y - x)\text{div } q$ ta có $y - x = B + dq$ và $yx = A - d$. Vậy

$$(B + dq)^2 + 4(A - d) = (y + x)^2,$$

tức (18) được thoả mãn.

Trường hợp $d \geq 0$ thì $B + dq \geq 0$ vậy

$$1 \leq \min(x, y) = 0.5(\sqrt{(B + dq)^2 + 4(A - d)} - (B + dq))$$

ta có

$$\begin{aligned} (B + dq)^2 + 4(A - d) &\geq (B + dq + 2)^2 \\ 4(A - d) &= 4(B + dq) + 4 \\ A - B - 1 &\leq d(q + 1) \text{ hay} \\ d &\leq (A - B - 1)div(g + 1) \end{aligned}$$

Trường hợp $d < 0$ thì $B + dq < 0$ vậy

$$1 \leq \min(x, y) = 0.5(\sqrt{(B + dq)^2 + 4(A - d)} + (B + dq))$$

ta có

$$\begin{aligned} (B + dq)^2 + 4(A - d) &\geq (2 - (B + dq))^2 \\ 4(A - d) &= 4 - 4(B + dq) \\ d(q - 1) &\leq -A - B + 1 \text{ hay} \\ d &\leq (-A - B + 1)div(g + 1). \end{aligned}$$

Kết hợp hai trường hợp trên ta có (17) được thoả mãn.

(b) $\Longrightarrow$ (a). Từ d thoả mãn (18) $(B + dq)^2 + 4(A - d) = C^2$ không giảm tổng quát giả sử $C \geq 0$. Ta đặt $x = 0.5(C - (B + dq))$ và $y = 0.5(C + (B + dq))$ khi đó rõ ràng ta có $x,\ y \geq 0$ và

$$\begin{aligned} (xq + 1)(yd - 1) &= xyq^2 + (y - x)q - 1 \\ &= = 0.25(C^2 - (B + dq)^2)q^2 + 0.5(2(B + dq))q - 1 \\ &= 0.25(4(A - d))q^2 + Bq + dq^2 - 1 \\ &= Aq^2 + Bq - 1 \\ &= N. \end{aligned}$$

Mặt khác từ điều kiện (17)

$$(-B - A + 1)\text{div}\ (q - 1) \leq d \leq (A - B - 1)\text{div}\ (q + 1).$$

ta có nếu $d < 0$ thì $y \leq x$ và

$$y = \min(x, y) = = 0.5(\sqrt{(B + dq)^2 + 4(A - d)} + (B + dq))$$

mà

$$\begin{aligned} d &\geq (-A - B + 1)\text{div}\ (q - 1) \\ d(q - 1) &\geq -A + B + 1 \\ 4(A - d) &\geq 4 - 4(B + dq) \\ (B + dq)^2 + (A - d) &\geq (2 - (B + dq))^2 \\ \sqrt{(B + dq)^2 + 4(A - d)} + (B + dq) &\geq 2, \end{aligned}$$

do đó $x, y \geq 1$. Trường hợp $d \geq 0$ ta cũng có lập luận tương tự và như vậy định lý đã được chứng minh.

Đến đây ta cũng rút ra một kết quả cuối cùng như sau:

Định lý 1.5. *Cho*

(i) $N = A2^{2k} + B2^k - 1$, *với* $k > 2$, $2||B$ *và* $0 < B < 2^k$.

(ii) $\{V_m\}$ *là dãy Lucas cuả phương trình* $x^2 - P\lambda + 1 = 0$ *thoả mãn điều kiện Riesel đối với* N.

Khi đó các điều kiện sau là tương đương:

(a) N *nguyên tố.*

(b) N *thoả mãn các điều kiện sau:*

(*) $V_{(N+1)/4} \equiv 0 \ mod \ N$

(**) Nếu $A > 0$ *thì với mọi* d *thoả mãn* $d_1 \leq d \leq d_2$ *với* $d_1 = (-B-A+1)div\,(2-1)$ *còn* $d_2 = 0$ *nếu* $A-B-1 < 0$ *và bằng* $(A-B-1)div\,(2^k+1)$ *nếu ngược lại thì* $(B+dq)^2+4(A-d)$ *không chính phương.*

Chứng minh. (a) $\Longrightarrow$ (b).

Nếu N nguyên tố từ định lý 3 ta có (*) thoả mãn, giả sử (**) không thoả mãn thì từ định lý 4 thì N phải là hợp số. Điều vô lý trên dẫn đến (**) phải được thoả mãn.

(b) $\Longrightarrow$ (a). Từ giả thiết điều kiện Riesel thoả mãn cùng với các điều kiện (*) nên giả thiết cuả định lý 3 được thoả mãn nên ta có mọi ước nguyên tố cuả N và do đó mọi ước cuả N đều có dạng $s2^k + 1$. Như vậy nếu N là hợp số thì $N = UV$ với $U = s2^k \pm 1$, $V = s'2^k - (\pm)1$ với $s, s' \geq 1$, lại theo định lý 4 ta có d thoả mãn $d_1 \leq d \leq d_2$ sao cho $(B + d2^k) + 4(A - d)$ chính phương, điều này mâu thuẫn với điều kiện (*) và do đó định lý đã được chứng minh.

Thuật toán kiểm tra tính nguyên tố kiểu $N + 1$

2.1. *Thuật toán.*

Định lý 1.5 trên là cơ sở thuật toán sau.

Thuật toán NT. Để kiểm tra tính nguyên tố cuả số N ta tiến hành qua các bước sau:

Bước 1: Biểu diễn $N = A2^{2k} + B2^k - 1$, với $2||B$, $0 < B < 2^k$.

Bước 2: Tìm phương trình trong điều kiện (ii) cuả định lý 5.

Bước 3: Kiểm tra điều kiện $V_{(N+1)/4} \equiv 0 \mathrm{mod}\ N$.

(*) Nếu sai kết luận N là hợp số, dùng chương trình

(*) Ngược lại kiểm tra điều kiện $A = 0$.

+ Nếu đúng kết luận N là nguyên tố, dùng chương trình.

+ Ngược lại sang bước 4.

Bước 4: Lần lượt kiểm tra tính chính phương cuả $S(d) = (B' + d2^k - 1)^2 + 4(A' - d)$ với d lần lượt từ d_1 đến d_2 với d_1, d_2 như trong định lý 1.5.

* Nếu đúng với một d nào đó thì kết luận N là hợp số, dùng chương trình.

* Ngược lại kết luận N là nguyên tố, dùng chương trình.

Nhận xét: Về nguyên tắc thì thuật toán nêu ở trên có thể kiểm tra tính nguyên tố cho một số lẻ mà với nó tồn tại phương trình thoả mãn Riesel. Chúng tôi sẽ chỉ ra các lớp số mà với chúng việc tìm phương trình thoả mãn điều kiện này có thể bằng cách tra bảng (điều kiện) tuy nhiên tính đa thức cuả nó vẫn không đạt được do bước 4. Ở đây chúng tôi sẽ đưa ra một lớp số cụ thể mà trên đó thuật toán NT dùng kiểm tra tính nguyên tố các số thuộc lớp đó sẽ đạt tính đa thức.

2.2. *Việc hạn chế lớp số*

Để thuật toán NT có thể thực hiện trong thời gian đa thức ta buộc phải hạn chế đối tượng đầu vào, việc hạn chế cụ thể được trình bày sau đây.

Đối với khó khăn gây ra bởi bước 2 ta chỉ xét lớp các số mà với chúng việc tìm phương trình đặc trưng thoả mãn điều kiện Riesel có thể thấy ngay. Sau đây sẽ đưa ra vài lớp số mà với chúng tôi cần thông qua một kiểm tra đơn giản ta có thể tìm được phương trình thoả màn điều kiện Riesel bằng cách tra bảng.

Điều kiện (*). Cho N có $J(D/N) = -1$. Khi đó phương trình đặc trưng $\lambda^2 - P\lambda + 1 = 0$ thoả mãn điều kiện Riesel có thể tìm được qua bảng sau

Bảng 2: Hệ số và nghiệm cuả phương trình thoả mãn điều kiện Riesel

D	4	nghiệm phương trình	b	r
3	4	$2 + \sqrt{3}$	$1 + \sqrt{3}$	2
5	3	$0.5\ (3 + \sqrt{5})$	$1 + \sqrt{5}$	4
11	22	$10 + 3\sqrt{11}$	$3 + \sqrt{11}$	2
13	11	$11 + 3\sqrt{13}$	$3 + \sqrt{13}$	4
17	66	$33 + 8\sqrt{17}$	$4 + \sqrt{17}$	1
19	340	$170 + 39\sqrt{19}$	$13 + 3\sqrt{19}$	2
29	27	$0.5(27 + \sqrt{29})$	$5 + \sqrt{29}$	4

Tất nhiên ta có thể làm tăng số lượng cuả bảng trên bằng cách dò tìm nhưng ở đây cũng nảy sinh vấn đề mà bài báo này chưa giải quyết được đó là:

Liệu có hay không phương trình thoả màn điều kiện Riesel đối với số N cho trước?

Tuy nhiên, ta có thể ta có thể suy ra được kết quả sau:

Định nghĩa 2.1. $LM = \{N$ lẻ: tồn tại $a \in [3;5;11;13;17;19;29]$ sao cho $J(a/N) = -1$ và $R \leq c'k^2$ với $N = R2^k - 1\}$.

Từ đó ta có:

Định lý 2.2. *Thuật toán NT là thuật toán kiểm tra nhanh tính nguyên tố các số lớp LM.*

Phần 3. Đánh giá về thuật toán *NT*3 và lớp số *LM*.

Hoàn toàn tương tự như ở mục 3 chương trước ta cũng thu được các kết luận sau:

3.1. *Đánh giá về lớp kiểm tra được*

Theo định lý Lucas ta thấy rằng lớp kiểm tra được cuả thuật toán NT là rộng hơn rất nhiều. Nếu như trong định lý Lucas yêu cầu đối với N phải là $\leq 2^{2k}$ thì ở thuật toán 6, N thậm chí có thể $> 2^{3k}$ với $N = R2^k - 1$, R lẻ. Đây là bước tiến khá lớn về mặt phát huy khả năng cuả các thuật toán kiểu $N+1$. Sau đây ta sẽ phân tích cụ thể một lớp con cuả lớp các số kiểm tra được cuả thuật toán NT.

Ký hiệu:

$$Ms = \{N = 12m - 5 | m \text{ lẻ}\}$$

và

$$Ms(k) = \{N = R2^k - 1 |\ R \text{lẻ } k > 2 \text{và } (-1)^k R = -1 \text{mod } 3\}$$

ta dễ dàng nhận được các kết quả sau:

Kết quả 3.1. $\{M_3(k)\}, k > 2$ là phân hoạch cuả M_3.

Kết quả 3.2. Hai phần tử kề nhau trong $M_3(k)$ cách nhau là 6.2^k.

Ký hiệu $LM_3 = \{N \in LM |\ J(3/N) = -1\}$, ta có kết quả sau:

Kết quả 3.3. Cho trước số $x > 0$ khi đó số các số N thuộc lớp LM_3 không quá $x (N \leq x)$ là $O(x^{2/3})$.

3.2. *Thời gian tính cuả thuật toán NT*

Người ta đã chỉ ra rằng thời gian tính cuả thủ tục tìm số Lucas thứ M là $O(m^5)$ và xác định tính chính phương cuả số M có thơi gian tính là $O(m^3)$ với $m = logM$. Trong thuật toán NT ta chỉ cần một lần tìm số Lucas thứ $(N+1)/4$ và đối với $N \in LM$ thì ta cần không quá C lần xác định tính chính phương cuả $S(d)$. Do vậy ta có

Định lý 3.4. *Thuật toán NT thực hiện trên lớp LM có thời gian tính là $O(n)$, ở đây $n = logN$, với N là đầu vào.*

3.3. *Kết quả thực hành*

Chúng tôi đã thể hiện thuật toán trên trong một bộ chương trình viết bằng ngôn ngữ TUBO-PASCAL, các kết quả thu được khi chạy chương trình như sau:

+ Đã tìm trong 95 lớp các số $LM_3(k)$, $k = 3...96$ và thấy rằng

* Luân tồn tại số nguyên tố trong các lớp đó.
* Có 21 lớp ngay số thứ nhất là nguyên tố.
* Có 55 lớp có số nguyên tố trong 9 số đầu cuả lớp
* Và lớp có số nguyên tố đầu tiên xa nhất là lớp $LM_3(51)$, nó là số thứ 70 cuả lớp.

Bảng 3. Số thứ tự cuả số nguyên tố đầu tiên cuả các lớp $LM_3(k)$ với k từ 3 cho đến 95.

k	t	k	t	k	t	k	t	k	t	k	t
3	1	19	1	35	5	51	70	67	8	83	16
4	1	20	3	36	3	52	11	68	30	84	15
5	1	21	2	37	6	53	32	69	10	85	31
6	3	22	11	38	2	54	1	70	8	86	51
7	11	23	3	39	5	55	9	71	13	87	33
8	1	24	14	40	18	56	54	72	1	88	24
9	2	25	11	41	4	57	10	73	16	89	1
10	1	26	2	42	9	58	13	74	19	90	18
11	5	27	21	43	14	59	20	75	5	91	21
12	1	28	11	44	6	60	3	76	5	92	40
13	1	29	2	45	2	61	1	77	10	93	49
14	1	30	7	46	4	62	9	78	8	94	11
15	9	31	1	47	6	63	11	79	13	95	9
16	3	32	1	48	1	64	13	80	19		
17	1	33	6	49	4	65	12	81	9		
18	1	34	21	50	2	66	16	82	24		

+ Đã kiểm tra 817 số ngẫu nhiên > 100 chữ số thập phân trong lớp LM_3 và thu được

* 10 số nguyên tố.
* Trong đó có 131 hợp số được phát hiện bởi việc kiểm tra $V_{(N+1)/4} \equiv 0 \bmod N$.
* Không có hợp số nào bị phát hiện bởi lọc chính phương.

+ Đã kiểm tra 306 mẫu số ngẫu nhiên có đúng 151 chữ số thập phân trong lớp LM và thu được

* 2 số nguyên tố.
* trong đó có 33 hợp số được phát hiện bởi việc kiểm tra $V_{(N+1)/4} \equiv 0 \bmod N$.
* không có hợp số nào thoả mãn $V_{(N+1)/4} \equiv 0 \bmod N$ nhưng bị phát hiện bởi lọc chính phương.

+ Đã kiểm tra 783 số ngẫu nhiên có 300 chữ số thập phân trong lớp LM và thu được

* 2 số nguyên tố.

* trong đó có 83 hợp số được phát hiện bởi việc kiểm tra $V_{(N+1)/4} \equiv \mathrm{mod} N$.

* không có hợp số nào thoả mãn $V_{(N+1)/4} \equiv 0 \mathrm{mod} N$ nhưng bị phát hiện bởi lọc chính phương.

Kết luận

Mặc dù các kết quả thu được về thuật toán kiểu $N+1$ cũng như các số kiểm tra được (lớp LM) cuả chúng tôi đưa ra trong bài báo này vẫn còn bị hạn chế rất nhiều nhưng dù sao với các kết quả thu được từ thực hành chúng ta hy vọng những kết quả trên sẽ cung cấp cho chúng ta một khả năng tạo lập nhanh kho số nguyên tố lớn.

Lời cảm ơn. Các kết quả trên dà được trình bày tại các xê mi na cuả Viện toán học và cuả bộ môn Toán học Viện kỹ thuật quân sự. Tác giả xin chân thành cảm ơn các thành viên tham gia về những ý kiến nhận xét quý báu giúp cho tác giả hoàn thiện các kết quả đạt được.

Tài liệu tham khảo

1. Allency L.B.J.T. and Redfern E.J., *Introduction to Number Theory with Computing,* Hodder and Shoughton, 1989.
2. Bach E., *Bounds for Primality Testing and related Problems,* Math. Comp. 55, 1990, n. 191.
3. Pomerance C., *Cryptology and Computational Number Theory,* Proc. Symp. Appl. Math. **42**, 1990.
4. Erdos P. and Pomerance C., *On the number of False Witnesses for a Composite Number,* Math. Comp. **46**, 1986.
5. Guy R.K., Lacampagne C.B. and Selfridge J.L., *Primes at Glance,* Math. Comp. **48**, 1987, 177.
6. Goldwasser S. and Kilian J., *Almost all primes can be quickly certified,* Laboratory for Computer Science Massachusetts Institute of Technology, 1986.
7. Ireland K. and Rosen M., *A classical introduction to Morden number theory,* Springer, 1982.
8. Su Hee Kim and Pomerance C., *The probability that a random probable prime is composite,* Math. Comp. **53**, 1989, 188.
9. Kranakis E., *Primality and Cryptography,* John Wiley and Sons, 1986.
10. Kurtz G.C., Shanks D. and Williams H.C., *Fast primality test for numbers less than* 50.10^9, Math. Comp., **46** 1983, 179.
11. Lidl R. and Niederreiter H. , *Finite fields,* Addison-Wesley, 1983.

12. Parady B.K., Smith J.F. and Zarantonello S., *Largest know twin primes,* Math. Comp. **55**, 1990, 191.
13. Pomerance C., *Very Short primality proof,* Math. Comp. **48**, 1987, 177.
14. Pintz J., Williams L.S. and Szemeredi E., *Infinite Sets of Primes with fast primality tests and quick generation of large primes,* Math. Comp. **53**, 1989, 157.
15. Pratchar K., *Verteilung der Prizahlen,* Springer, 1957.
16. Ribenboim P., *The little book of big primes,* 1991.
17. Riesel H., *Prime number and computer methods for factorization,* Progress in Math. **57**, 1985.
18. Salomaa A., *Public-key cryptography,* EATCS, 1990.
19. Williams H.C., *Primality testing on a computer,* Ars Combin, 5, 1978.
20. Williams H.C. and Zarnke C.R., *Some prime numbers of the forms* $2A3^n + 1$ *and* $2A3^n - 1$, Math. Comp. **26**, 1972, 120.

Abstract

Extension of class of Mersenn's numbers

In this paper we investigate a class of nature numbers denoted by LM which properly includes the class of Mersenn ones. For this class, we propose an algorithm for testing primality. The algorithm works in polynomial time according to input belonging to LM.

The problem that whether or not LM contains infinitely-many primes, even under the generalized Riemann hypothesis is open one.