Podiplomski študij matematike, raziskovalna smer

Kriptografija

Testiranje praštevilskosti

Gregor Šega

1 Fermatov test

V kriptografiji so praštevila pomemben dejavnik. Mnogo algoritmov vsebuje stavek kot "izberimo stomestno praštevilo". Stomestnih praštevil je preveč, da bi jih imeli spravljene v neki datoteki, ter bi jih naključno črpali iz nje. Zato si v praksi izmislimo neko število, in nato preverimo, če je res praštevilo. Če namreč kriptografski sistem izrablja lastnosti praštevil, nam sestavljeno število namesto praštevila pomeni visoko tveganje za varnost, lahko pa se celo zgodi, da šifriranje ali dešifriranje sploh ni mogoče. V $\mathbb{Z}_n^*$ mnogo elementov sploh ni obrnljivih, če n ni praštevilo. Zato potrebujemo močne algoritme, ki nam povedo, če je izbrano število sestavljeno ali ne.

Izrek 1. (Fermat)
Naj bo p praštevilo in a poljubno celo število. Potem velja $a^p \equiv a (\mathrm{mod}\ p)$.

Dokaz. Očitno izrek velja za $a = 1$. Recimo, da velja za nek a. Potem je

$$(a+1)^p \equiv a^p + 1 (\mathrm{mod}\ p) \equiv a + 1 (\mathrm{mod}\ p).$$

Prva enakost velja, ker je $\binom{p}{k}$ deljiv s p za $k = 1, \ldots, p-1$, druga enakost pa velja po indukcijski predpostavki.

Ta izrek lahko uporabimo kot dokaz, da je izbrano število n sestavljeno število. Izberemo si nek a, izračunamo $a^n (\mathrm{mod}\ n)$ in rezultat primerjamo z a. Če rezultat ni enak a, imamo dokaz, da n ni praštevilo. Ta test je dovolj močan. Recimo za $a = 2$ je prvo število, ki je sestavljeno, pa vseeno velja $2^n \equiv 2$, število 341. Če test ponovimo poleg števila 2 še s števili 3, 5 in 7, je do $25 \cdot 10^9$ le 1770 števil, ki nas prevarajo. To število ni preveliko, je pa dovolj veliko, da nas resno zmoti. Poleg tega se vprašamo, če obstajajo sestavljena števila, za katere priče sploh ne obstajajo, torej velja $a^n \equiv a (\mathrm{mod}\ n)$ za vsak a. Že leta 1899 je Korselt karakteriziral ta števila.

Izrek 2. (Korselt, 1899)
Naj bo n sestavljeno število. Potem velja $a^n \equiv a(\mathrm{mod}\ n)$ za vsak a natanko tedaj, ko je n brez kvadratov in za vsako praštevilo p, ki deli n, velja $p-1|n-1$.

Dokaz. Naj bo najprej $a^n \equiv a(\mathrm{mod}\ n)$ za vsak a. Naj bo p nek praštevilski delitelj števila n. Recimo, da tudi p^2 deli n. Za število a si izberimo kar p. Torej n deli $p^n - p$ in zato tudi p^2 deli $p^n - p$. To pa pomeni, da p deli $p^{n-1} - 1$, kar pa ni mogoče. p^2 torej ne deli števila n.
Naj bo p kot prej nek praštevilski delitelj števila n. Zapišemo lahko torej $n = p \cdot m$. Sedaj $n-1$ delimo s $p-1$ in dobimo $n - 1 = (p-1) \cdot k + o$, $0 \leq o < p - 1$. Radi bi ugotovili, koliko je ostanek o. Izberimo si a, ki naj bo generator $\mathbb{Z}_p^*$. Po predpostavki velja

$$p \cdot m \cdot \alpha = a^{p \cdot m} - a = a(a^{(p-1)k+o} - 1).$$

Poglejmo to enakost po modulu p:

$$0 \equiv a(1^k \cdot a^o - 1)(\mathrm{mod}\ p).$$

Upoštevali smo, da je p praštevilo, in torej velja $a^{p-1} \equiv 1(\mathrm{mod}\ p)$. Na koncu smo dobili

$$a \equiv a^{o+1}(\mathrm{mod}\ p),$$

kar pomeni, da je $o + 1 \equiv 1(\mathrm{mod}\ p-1)$ (ker je a generator $\mathbb{Z}_p^*$). Ker pa je o med 0 in $p-2$, mora biti $o = 0$, torej $p-1$ res deli $n-1$.
Poglejmo sedaj še obrat. Število n naj bo oblike

$$n = p_1 \cdot p_2 \cdots p_k,$$

kjer so p_i različna praštevila, in naj $p_i - 1$ deli $n-1$ za vsak i. Vzemimo poljuben a in izračunajmo $a^n - a(\mathrm{mod}\ n)$. Poglejmo najprej, koliko je $a^n - a(\mathrm{mod}\ p_i)$ za nek i:

$$a^n - a = a \cdot a^{n-1} - a = a \cdot a^{(p_i-1)\frac{n-1}{p_i-1}} - a =$$
$$= a \cdot (a^{p_i-1})^{\frac{n-1}{p_i-1}} - a \equiv a \cdot 1^{\frac{n-1}{p_i-1}} - a(\mathrm{mod}\ p_i) \equiv a - a(\mathrm{mod}\ p_i) \equiv 0(\mathrm{mod}\ p_i).$$

To pomeni, da je $a^n - a$ deljivo z vsemi p_i, torej tudi z n.

Kot rečeno, je Korselt ta izrek dokazal že leta 1899. Vendar pa je on podvomil v obstoj takih števil, njegova ugotovitev se mu je zdela brez vrednosti. Leta 1910 je Carmichael ugotovil, da velja $561|a^{561} - a$ za vsak a. Po Korseltovem kriteriju hitro preverimo, da to drži: $561 = 3 \cdot 11 \cdot 17$ in 560 je deljivo z 2, 10 in 16. Oglejmo si sedaj nekaj lastnosti Carmichaelovih števil.

Posledica 1. Carmichaelovo število je liho in ima vsaj tri praštevilske delitelje.

Dokaz. Recimo, da je n sodo. V tem primeru je $n-1$ liho, in ker ima n vsaj enega lihega delitelja p , $p-1$, ki je sodo število, ne deli $n-1$.
Naj bo $n = p \cdot q$. Potem $p-1$ deli $pq-1$, prav tako $q-1$ deli $pq-1$. Ker pa $p-1$ jasno deli $pq-q$, deli tudi $q-1$, prav tako $q-1$ deli $p-1$. Torej je $p-1 = q-1$ oziroma $p = q$, kar pa ni možno.

Obstajajo pa Carmichaelova števila, ki imajo štiri, pet, šest, ... deliteljev. Nekatera Carmichaelova števila lahko poiščemo precej enostavno:

Posledica 2. Če so $6n+1$, $12n+1$ in $18n+1$ praštevila, je njihov produkt Carmichaelovo število.

Dokaz. Izračunati moramo le

$$(6n+1)(12n+1)(18n+1)-1 = 1296n^3+396n^2+36n = 36n(36n^2+11n+1).$$

To število je jasno deljivo s $6n$, $12n$ in $18n$.

Vemo, da je v vsakem aritmetičnem zaporedju, ki vsebuje vsaj en lih člen, neskončno praštevil. Dickson je leta 1904 postavil hipotezo, da celo če imamo več takih zaporedij $\{a_1 \cdot n+b_1\}$, $\{a_2 \cdot n+b_2\}$, ..., $\{a_k \cdot n+b_k\}$, obstaja neskončno indeksov n, za katere so ustrezni členi zaporedij vsi hkrati praštevila (razen, če očitno ne morejo biti, kar pomeni, da obstaja praštevilo, ki za vsak n deli njihov produkt). Ta hipoteza se zdi "precej verjetna", dokazana (ali ovržena) pa še ni. Ob privzetku Dicksonove hipoteze so $6n+1$, $12n+1$ in $18n+1$ praštevila za neskončno n-jev, kar pomeni, da je Carmichaelovih števil neskončno mnogo.

S pomočjo posledice 2 lahko poiščemo precej velika Carmichaelova števila. Zelo slab računalnik (a tako dober, da na njem lahko uporabljamo Mathematico), najde stoenamestno Carmichaelovo število

$$11856311014966876020020515407623 47\cdot$$

$$23712622029933752040041030815246 93\cdot$$

$$35568933044900628060061546222870 39 =$$

$$10000000000000000000000000000040 59 \setminus \setminus$$

$$29367865700162694655745350302085 8 \setminus \setminus$$

$$10080768959837103297359653235421369$$

v nekaj minutah, dvestoenamestno Carmichaelovo število pa v pol ure:

$$25543647746451770219954184281098639478619802270452614111983677714370\cdot$$

$$51087295492903540439908368562197278957239604540905228223967355428730\cdot$$

$$76630943239355310659862552843295918435859406811357842335951033143090 =$$

$$10000000000000000000000000000000000000000000000000\,\backslash\backslash$$

$$00000000021668584048317666988783265106818258987940\,\backslash\backslash$$

$$39181125349720831699052655159251071979853867986464\,\backslash\backslash$$

$$33101380449439432244827726029100253226539451273080 9$$

Trenutno največje Carmichaelovo število te oblike ime 4848 mest, dobimo pa ga pri

$$n = 133752260 \cdot 3003 \cdot 10^{1604}.$$

Že Carmichael je leta 1910 domneval, da je teh števil neskončno mnogo, vendar pa je to ostala odprta hipoteza do leta 1994, ko so Alford, Granville in Pomerance dokazali, da je Carmichaelovih števil neskončno. Natančneje, dokazali so, da je teh števil, manjših od x, vsaj $x^{2/7}$ (za dovolj velike x). Kot kaže iz dokaza izreka, je prava meja verjetno kar $x^{1-o(x)}$.

Za predstavo, kako redka so Carmichelova števila, si oglejmo nekaj najmanjših: 561, 1105, 1729, 2465, 2821, ... Do milijona jih najdemo le 43, do $25 \cdot 10^9$ jih je 2163, do 10^{16} pa 246683. Vsa ta števila so znana in zbrana v tabelah. Največje do sedaj znano Carmichaelovo število nasploh ima 10200 mest (in je produkt treh praštevil), največje Carmichaelovo število s štirimi faktorji je 2467-mestno, s petimi 1015-mestno in s šestimi 827-mestno. Se pa ti rekordi spreminjajo skoraj vsakodnevno, saj procesorske moči računalnikov še kar rastejo, prav tako pa se razvijajo tudi algoritmi.

Fermatov test je sicer močan, žal pa se mu Carmichaelova števila izmuznejo. Zato je bilo potrebno razviti boljše algoritme, ki sestavljenih števil ne bi proglasili za praštevila. Sedaj se najbolj uporabljajo Solovay-Strassnov algoritem, Miller-Rabinov test in Lucasov test. Vendar pa za vsak do sedaj znan test obstaja množica števil, ki jih ta test ne identificira pravilno. Vsi ti testi so namreč pristranski. Če odgovorijo, da je število sestavljeno, imajo dokaz za tako trditev, če pa odgovorijo, da je število praštevilo, to pomeni, da niso našli nobenega dokaza, ki bi nam potrdil, da je število sestavljeno. So pa testi sestavljeni tako, da so sestavljena števila, ki se obnašajo popolnoma enako kot praštevila, precej redka. Zato se sedaj v praksi (recimo v `Mathematici`) uporablja kombinacija

testov. Tako (morda) dobimo resničen odgovor. Recimo, `Mathematica` pri testu praštevilskosti najprej testira deljivost s praštevili pod 373, nato naredi Miller-Rabinov test, na koncu (če še ni našla dokaza, da je število sestavljeno), pa še Lucasov test.

Obstaja pa nekaj algoritmov, ki nam (ob določenih predpostavkah) dokažejo, da je število praštevilo. Prvi primer je Lehmerjev obrat Fermatovega izreka:

Izrek 3. Naj bo $n-1 = \prod_{j=1}^{k} q_j^{\beta_j}$, kjer so q_j različna praštevila. Če obstaja celo število a, za katerega velja

$$a^{(n-1)/q_j} \not\equiv 1 (\mathrm{mod}\ n), \qquad \text{za vse } j = 1, 2, \ldots, k$$

in

$$a^{n-1} \equiv 1 (\mathrm{mod}\ n),$$

potem je n praštevilo.

Dokaz. Ta izrek je ekvivalenten naslednji trditvi:
Naj bo n kot v izreku, in naj bo praštevilo. Potem je a generator grupe $\mathbb{Z}_n^*$ natanko tedaj, ko velja

$$a^{(n-1)/q_j} \not\equiv 1 (\mathrm{mod}\ n), \qquad \text{za vse } j = 1, 2, \ldots, k$$

Če je namreč n praštevilo, ima grupa $\mathbb{Z}_n^*$ generator a, za katerega pa pogoja iz izreka veljata. Če pa obstaja tak a, je generator grupe $\mathbb{Z}_n^*$, to pa pomeni, da je n praštevilo.

Dokažimo še trditev o generatorju:
Če je a generator, je $a^0 \equiv 1$ in zato $a^{\frac{n-1}{q_i}} \not\equiv 1$. Če a ni generator, obstaja c, $0 < c < n-1$, da je $a^c \equiv 1$. Izberimo najmanjši tak pozitiven c. Torej je tudi $a^{cj} \equiv 1$, za vsak j. Recimo, da je $cj < n-1 < c(j+1)$. Potem je $a^{cj} \equiv 1 \equiv a^{n-1}$ in zato $a^{n-1-cj} \equiv 1$, kar je protislovje, saj je $0 < n-1-cj < c$. Torej je $cj = n-1$ za nek j, oziroma j deli $n-1$. Potem pa je j deljiv z nekim q_i, torej $j = q_i \cdot x$. Imamo torej $1 \equiv \alpha^{cx} = \alpha^{cj/q_i} = \alpha^{\frac{n-1}{q_i}}$.

Ta izrek nam pove, da lahko dokažemo, da je n praštevilo, če poznamo faktorizacijo števila $n-1$. Tega pa mnogokrat ne poznamo, zato izrek nima splošne velike vrednosti. Je pa zelo uporaben za določene skupine števil.

Primer. Dokažimo, da je $2^{16}+1$ praštevilo, $2^{32}+1$ pa ne.
Ti števili sta znani Fermatovi števili F_4 in F_5. Fermat je postavil hipotezo, da so števila oblike $F_n = 2^{2^n}+1$ praštevila. Trenutno vemo, da so števila F_0 do

F_4 praštevila, števila F_5 do F_8 so popolnoma razcepljena (razcepe so našli v letih 1732, 1880, 1974, 1980), dokazano sestavljena števila so do F_{19}, nekateri faktorji pa so znani celo za število F_{23471}; to število je približno 10^{8000}-mestno!
Naj bo najprej $n = 2^{16} + 1 = 65537$. Faktorizacija števila $n - 1$ je potem precej enostavna, izvede naj jo bralec sam. Izberimo si $a = 3$ in izračunajmo

$$3^{2^1} \equiv 9 (\mathrm{mod}\ 65537), \qquad 3^{2^2} \equiv 81 (\mathrm{mod}\ 65537),$$

$$3^{2^3} \equiv 6561 (\mathrm{mod}\ 65537), \qquad 3^{2^4} \equiv 54449 (\mathrm{mod}\ 65537),$$

$$3^{2^5} \equiv 61869 (\mathrm{mod}\ 65537), \qquad 3^{2^6} \equiv 19139 (\mathrm{mod}\ 65537),$$

$$3^{2^7} \equiv 15028 (\mathrm{mod}\ 65537), \qquad 3^{2^8} \equiv 282 (\mathrm{mod}\ 65537),$$

$$3^{2^9} \equiv 13987 (\mathrm{mod}\ 65537), \qquad 3^{2^{10}} \equiv 8224 (\mathrm{mod}\ 65537),$$

$$3^{2^{11}} \equiv 65529 (\mathrm{mod}\ 65537), \qquad 3^{2^{12}} \equiv 64 (\mathrm{mod}\ 65537),$$

$$3^{2^{13}} \equiv 4096 (\mathrm{mod}\ 65537), \qquad 3^{2^{14}} \equiv 65281 (\mathrm{mod}\ 65537),$$

$$3^{2^{15}} \equiv 65536 (\mathrm{mod}\ 65537), \qquad 3^{2^{16}} \equiv 1 (\mathrm{mod}\ 65537).$$

To dokazuje, da je 65537 praštevilo.
Enake izračune ponovimo za $n = 2^{32} + 1 = 4294967297$:

$$3^{2^1} \equiv 9 (\mathrm{mod}\ 4294967297), \qquad 3^{2^2} \equiv 81 (\mathrm{mod}\ 4294967297),$$

$$3^{2^3} \equiv 6561 (\mathrm{mod}\ 4294967297), \qquad 3^{2^4} \equiv 43046721 (\mathrm{mod}\ 4294967297),$$

$$3^{2^5} \equiv 3793201458 (\mathrm{mod}\ 4294967297), \qquad 3^{2^6} \equiv 1461798105 (\mathrm{mod}\ 4294967297),$$

$$3^{2^7} \equiv 852385491 (\mathrm{mod}\ 4294967297), \qquad 3^{2^8} \equiv 547249794 (\mathrm{mod}\ 4294967297),$$

$$3^{2^9} \equiv 1194573931 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{10}} \equiv 2171923848 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{11}} \equiv 3995994998 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{12}} \equiv 2840704206 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{13}} \equiv 1980848889 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{14}} \equiv 2331116839 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{15}} \equiv 2121054614 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{16}} \equiv 2259349256 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{17}} \equiv 1861782498 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{18}} \equiv 1513400831 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{19}} \equiv 2897320357 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{20}} \equiv 367100590 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{21}} \equiv 2192730157 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{22}} \equiv 2050943431 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{23}} \equiv 2206192234 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{24}} \equiv 2861695674 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{25}} \equiv 2995335231 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{26}} \equiv 3422723814 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{27}} \equiv 3416557920 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{28}} \equiv 3938027619 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{29}} \equiv 2357699199 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{30}} \equiv 1676826986 (\mathrm{mod}\ 4294967297),$$

$$3^{2^{31}} \equiv 10324303 (\mathrm{mod}\ 4294967297), \qquad 3^{2^{32}} \equiv 3029026160 (\mathrm{mod}\ 4294967297).$$

To dokazuje, da 4294967297 ni praštevilo.

Izkaže se, da je v splošnem primeru dovolj preveriti le za $a = 3$:

Izrek.(Pepin) Potreben in zadosten pogoj za to, da je število $2^{2^n}+1$ praštevilo, je to, da velja

$$3^{2^{2^n-1}} \equiv -1 (\mathrm{mod}\ 2^{2^n}+1).$$

Bistvo dokaza. Na pomoč prikličemo teorijo kvadratičnih ostankov. Hitro preverimo, da 3 ni kvadratični ostanek nad $2^{2^n}+1$, od tod pa izpeljemo dokaz.

2 Lucasov test

Naj bosta P in Q celi števili. Korena enačbe

$$x^2 - Px + Q = 0$$

označimo z a in b. Lahko ju tudi izračunamo:

$$a = \frac{1}{2}(P + \sqrt{D}),$$

$$b = \frac{1}{2}(P - \sqrt{D}),$$

pri čemer je

$$D = P^2 - 4Q.$$

Za a in b veljajo zveze

$$a + b = P,$$

$$ab = Q,$$

$$a - b = \sqrt{D}.$$

Z a in b definiramo dve Lucasovi zaporedji:

$$U_n(P,Q) = \frac{a^n - b^n}{a - b},$$

$$V_n(P,Q) = a^n + b^n.$$

Prvih nekaj vrednosti je enakih

$$U_0(P,Q) = 0, \qquad V_0(P,Q) = 2,$$

$$U_1(P,Q) = 1, \qquad V_1(P,Q) = P.$$

Za zaporedji U_n in V_n veljajo naslednje rekurzivne relacije:

$$U_{n+m} = \frac{a^{n+m} - b^{n+m}}{a-b} =$$

$$= \frac{(a^n - b^n)(a^m + b^m)}{a-b} - \frac{a^m b^m (a^{n-m} - b^{n-m})}{a-b} =$$

$$= U_n V_m - Q^m U_{n-m},$$

$$V_{n+m} = a^{n+m} + b^{n+m} =$$

$$= (a^n + b^n)(a^m + b^m) - a^m b^m (a^{n-m} + b^{n-m}) =$$

$$= V_n V_m - Q^m V_{n-m}.$$

Za poseben primer $m = 1$ dobimo

$$U_{n+1} = PU_n - QU_{n-1},$$

$$V_{n+1} = PV_n - V_{n-1}.$$

S tem smo dokazali, da sta zaporedji U in V celoštevilski.
Recimo, za $P = 1$ in $Q = -1$ je U znano Fibonaccijevo zaporedje, V pa mnogokrat imenujejo Lucasovo zaporedje (prva člena sta 2 in 1, rekurzivna enačba pa je enaka kot pri Fibonaccijevem zaporedju).
Vzemimo sedaj v rekurzivnih enačbah $m = n$ in $n = m + 1$:

$$U_{2n} = U_n V_n,$$

$$V_{2n} = V_n^2 - 2Q^n,$$

$$U_{2m+1} = U_{m+1} V_m - Q^m,$$

$$V_{2m+1} = V_{m+1} V_m - PQ^m.$$

S pomočjo teh formul lahko izračunamo člene U_n in V_n v logaritemskem času, pri čemer moramo voditi samo štiri količine.

Primer. Recimo, da želimo izračunati U_{100} (za $(P, Q) = (1, -1)$): veljajo formule

$$U_{100} = U_{50} V_{50}, \qquad V_{100} = V_{50}^2 - 2,$$
$$U_{50} = U_{25} V_{25}, \qquad V_{50} = V_{25}^2 + 2.$$

Sedaj uporabimo predpis za lihe indekse:

$$U_{25} = U_{13} V_{12} - 1, \qquad V_{25} = V_{13} V_{12} - 1.$$

Kot kaže, se bo število členov, ki jih moramo izračunati, od sedaj naprej podvojevalo. Na srečo to ni res:

$$U_{13} = U_7V_6 - 1, \qquad V_{13} = V_7V_6 - 1,$$

$$U_{12} = U_6V_6, \qquad V_{12} = V_6^2 - 2.$$

Spet imamo le štiri količine. Naslednji koraki so potem

$$U_7 = U_4V_3 + 1, \qquad V_7 = V_4V_3 + 1,$$

$$U_6 = U_3V_3, \qquad V_6 = V_3^2 + 2;$$
$$U_4 = U_2V_2, \qquad V_4 = V_2^2 - 2,$$
$$U_3 = U_2V_1 + 1, \qquad V_3 = V_2V_1 + 1;$$
$$U_2 = U_1V_1, \qquad V_2 = V_1^2 + 2.$$

Upoštevamo še $U_1 = V_1 = 1$, pa dobimo

$$U_2 = U_1V_1 = 1, \qquad V_2 = V_1^2 + 2 = 3,$$

$$U_3 = U_2V_1 + 1 = 2, \qquad V_3 = V_2V_1 + 1 = 4,$$
$$U_4 = U_2V_2 = 3, \qquad V_4 = V_2^2 - 2 = 7,$$
$$U_6 = U_3V_3 = 8, \qquad V_6 = V_3^2 + 2 = 18,$$
$$U_7 = U_4V_3 + 1 = 13, \qquad V_7 = V_4V_3 + 1 = 29,$$
$$U_{12} = U_6V_6 = 144, \qquad V_{12} = V_6^2 - 2 = 322,$$
$$U_{13} = U_7V_6 - 1 = 233, \qquad V_{13} = V_7V_6 - 1 = 521,$$
$$U_{25} = U_{13}V_{12} - 1 = 75025, \qquad V_{25} = V_{13}V_{12} - 1 = 167761,$$
$$U_{50} = U_{25}V_{25} = 12586269025, \qquad V_{50} = V_{25}^2 + 2 = 28143753123,$$
$$U_{100} = U_{50}V_{50} = 354224848179261915075.$$

Dejstvo, da se da člene zaporedja U (in seveda tudi zaporedja V) učinkovito izračunati, potrebujemo zaradi naslednje trditve:

Izrek 5. Naj bo $n \geq 2$, $P^2 - 4Q = c^2 D$, D pa je brez kvadratov. Naj bo p praštevilo. Potem velja: če sta p in $2QD$ tuji števili, je

$$U_{p^{n-1}(p-(\frac{D}{p}))} \equiv 0 (\text{mod } p^n).$$

Dokaz. (Spet le skica) Najprej dokažemo Fermatov izrek za obseg $\mathbb{Z}[\sqrt{D}] = \{k + l\sqrt{D}; k, l \in \mathbb{Z}\}$:

$$a^p \equiv a (\text{mod } p), \qquad \text{če } \left(\frac{D}{p}\right) = 1,$$

$$a^p \equiv \overline{a} (\text{mod } p), \qquad \text{če } \left(\frac{D}{p}\right) = -1.$$

Pri tem je $\left(\frac{D}{p}\right)$ Jacobijev simbol. Potem Fermatov izrek uporabimo za a in b in dobimo želeni rezultat.

Ker pri dokazovanju, da je n praštevilo (z Lehmerjevim preskusom) potrebujemo faktorizacijo števila $n-1$, ki pa je nimamo, nam prav pride Lucasov test, natančneje Lucas-Lehmerjev test, za katerega potrebujemo faktorizacijo $n+1$.

Izrek 6. Naj bo $n + 1 = \prod_{j=1}^{k} q_j^{\beta_j}$, kjer so q_j različna praštevila. Če obstaja Lucasovo zaporedje $\{U_i\}$, za katerega velja $(2QD, n) = 1$,

$$(U_{(n+1)/q_j}, n) = 1 \qquad \text{za vse } j = 1, 2, \ldots, k,$$

in

$$U_{n+1} \equiv 0 (\text{mod } n),$$

potem je n praštevilo.

Ta test je najbolj uporaben pri Mersenne-ovih številih $M_p = 2^p - 1$, saj moramo v tem primeru preveriti najmanj pogojev. S tem testom dandanes odkrivajo največja praštevila. Trenutno je znanih 37 praštevil zgornje oblike, največje med njimi je $2^{3021377} - 1$, kar pomeni, da je 909526 mestno! Za konec navedimo še posebno obliko izreka 6 za Mersennova števila:

Izrek 7. Naj bo $M_p = 2^p - 1$. M_p je praštevilo natanko tedaj, ko M_p deli s_{p-2}, pri čemer je $s_0 = 4$ in $s_{i+1} = s_i^2 - 2$.

Literatura:

1. Hans Riesel: Prime numbers and computer methods for factorization, Birkhäuser, 1985

2. W.R. Alford, A. Granville, C. Pomerance: There are infinitely many Carmichael numbers, Ann. Math., 140(1994), 703-722

3. E. Bach, J. Shallit: Algoritmic Number Theory, Volume I: Efficient Algorithms, MIT Press, 1996

4. H. Cohen: A Course in Computational Algebraic Number Theory, Springer, 1993

5. Number theorists uncover a slew of prime impostors, What's happening in the mathematical sciences, 1994

6. Stephan Wolfram: The Mathematica book, 3rd edition

7. The Largest Known Prime Number,
`http://www.math.utah.edu/~alfeld/math/largeprime.html`

8. Dickson's conjecture,
`http://www.utm.edu/research/primes/glossary/DicksonsConjecture.html`

9. E.W. Weisstein, CRC Concise Encyclopedia of Mathematics, CRC Press, 1998
`http://www.astro.virginia.edu/ eww6n/math/`