MMG100 - Elementär talteori
Primtalstester

Anders Martinsson

Ett *primalitetstest* eller *primtalstest* är ett test för att avgöra om ett givet positivt heltal n är ett primtal eller inte. Det första primtalstestet vi har sett i kursen bygger på Proposition 1.7 i kursboken: varje sammansatt tal n har en primtalsdelare $p \leq \sqrt{n}$. Detta innebär att om vi vill testa om ett heltal $n > 1$ är ett primtal så räcker det att se om n är delbart med något primtal upp till $\sqrt{n}$. Om n är "rimligt litet" kan detta utföras snabbt med papper och penna. Med hjälp av dator denna metod utföras på rimlig tid för heltal n upp till $\approx 10^{18}$, dvs. 17–18–siffriga tal.

Exempel. Avgör om 119 och 127 är primtal.

> Vi konstaterar först att 119 ligger mellan $10^2 = 100$ och $11^2 = 121$. Därmed är $10 < \sqrt{119} < 11$. Det räcker att se om 119 är delbart med något primtal ≤ 10. Efter lite räknande kan vi se att $119/7 = (70 + 49)/7 = 17$ så 119 är delbart med 7. Vi ser att $119 = 7 \cdot 17$ inte är ett primtal.
>
> På samma sätt, 127 ligger mellan $11^2 = 121$ och $12^2 = 144$, så det räcker att testa delbarhet med primtal $p \leq 11$. Efter lite räknande med papper och penna kan vi konstatera att 127 varken är delbart med 2, 3, 5, 7 eller 11, så vi kan dra slutsatsen att 127 är ett primtal.

En mycket viktig tillämpning av primtalstester är för att generera nycklar till RSA-kryptering. Kom ihåg att första steget till att skapa en RSA-nyckel är att generera två stora primtal. I praktiken kan "stora" här innebära att primtalen skall vara upp till flera hundra siffror långa. För att kunna hitta sådana primtal behövs primtalstest som kan utföras på rimlig tid för tal med hundratals siffror. I det här fallet är testet vi beskriver ovan helt oandvändbart, utan andra snabbare metoder behövs. Nedan kommer vi beskriva två sådana metoder, båda baserade på Fermats lilla sats.

Fermats primtalstest

Låt n vara ett positivt heltal större än 1, och låt $a = 2, 3, \ldots, n-1$. Enligt Fermats lilla sats vet vi att om n är ett primtal, så är

$$a^{n-1} \equiv 1 \bmod n. \tag{1}$$

Omvänt, givet ett positivt heltal n, om vi väljer ett heltal a mellan 2 och $n-1$ och det visar sig att $a^{n-1} \not\equiv 1 \bmod n$ kan vi dra slutsatsen att n inte är ett primtal. Detta kallas för Fermats primtalstest.

Här bör det påpekas att exponenter a^m mod n kan beräknas snabbt mha dator, men detta kommer vi inte diskutera i kursen. Den intresserade läsaren kan t.ex. se studentprojekt 1 i kapitel 2 av kursboken.

Exempel. Använd Fermats primtalstest för att visa att 15 inte är ett primtal.

> Låt oss välja $a = 2$. Vi har $2^{14} = 16384$ vilket har rest 4 vid division med 15. Därmed är $2^{14} \equiv 4 \not\equiv 1 \bmod n$, och vi kan dra slutsatsen att 15 ej är ett primtal.

Observera från exemplet att vi kunde se att 15 är ett sammansatt tal utan att se hur 15 kan faktoriseras. Detta är en gemensam egenskap av alla kända "effektiva" primtalstester. Förvånansvärt nog är det betydligt svårare att faktorisera vissa tal än vad det är att testa om de är primtal.

Om $a^{n-1} \not\equiv 1 \bmod n$ kan vi alltså dra slutsatsen att n är ett sammansatt tal. Vad kan vi dra för slutsats om $a^{n-1} \equiv 1 \bmod n$? Det är kanske lockande tro att n är måste vara ett primtal, men detta är desvärre inte sant. Exempelvis är

$$2^{341-1} \equiv 1 \bmod 341,$$

men $341 = 11 \cdot 31$ är ett sammansatt tal, och

$$3^{91-1} \equiv 1 \bmod 91,$$

men $91 = 7 \cdot 13$ är också ett sammansatt tal. Ett sammansatt tal som "lurar" Fermats test på det här sättet för ett givet a kallas for *pseudoprimtal* i bas a, dvs 341 är ett pseudoprimtal i bas 2 och 91 är ett pseudoprimtal i bas 3.

I vissa fall kan vi se om ett tal är ett pseudoprimtal genom att utföra Fermats test för flera val av a, men detta är inte alltid tillräckligt. Exempelvis har $561 = 3 \cdot 11 \cdot 17$ egenskapen att

$$a^{561-1} \equiv 1 \bmod 561$$

för alla a som är relativt prima 561. Ett sammansatt tal n med denna egenskap är ett *Carmichaeltal*. Det är känt att det finns oändligt många Charmichaeltal (och därmed även oändligt många pseudoprimtal), och det finns anledning att tro att sådana tal är ganska vanliga.

En styrka med Fermats primtalstest är vi i många fall snabbt kan konstatera att ett tal n är ett sammansatt tal. En stor svaghet är dock att det finns oändligt många s.k. pseudoprimtal som testet inte kan särskilja från primtal. Så vi aldrig kan vara riktigt säkra på att ett tal vi har hittat är ett primtal.

Miller–Rabins primtalstest

Miller–Rabins primtalstest är en förfining av Fermats test som till stor del löser problemen med pseudoprimtal. Låt n vara ett heltal större än 1, och låt a vara ett heltal mellan 2 och $n - 1$. Här antar vi att n är udda (primtalstest för jämna tal är enkelt). Enligt Fermats lilla sats vet vi att om n är ett primtal så är

$$a^{n-1} - 1 \equiv 0 \bmod n. \tag{2}$$

För att illustrera idén med Miller–Rabins test, låt oss som ett exempel ta $n = 21$. (Vi låtsas att vi inte har någon aning om huruvida 21 är ett primtal.) Genom upprepad användning av konjugatregeln får vi

$$\begin{aligned} a^{20} - 1 &\equiv (a^{10} - 1)(a^{10} + 1) \\ &\equiv (a^5 - 1)(a^5 + 1)(a^{10} + 1) \bmod 21. \end{aligned}$$

Om 21 är ett primtal skall detta vara kongruent med 0. Det gäller allmänt att om en produkt är kongruent med 0 modulo ett primtal, så är någon av faktorerna kongruent med 0 (detta är en följd av Euklides lemma 1.14 i boken). Så om 21 är ett primtal måste antingen $a^5 \equiv \pm 1 \bmod 21$ eller $a^{10} \equiv -1 \bmod 21$.

Om vi till exempel väljer $a = 2$ får vi $a^5 = 32 \equiv 11 \not\equiv \pm 1 \bmod 21$ och $a^{10} = 1024 \equiv 16 \not\equiv -1 \bmod 21$. Då inget av villkoren är uppfyllda kan vi dra slutsatsen att 21 inte är ett primtal.

Mer allmänt är Miller–Rabins primtalstest som följer. Vi har givet n, ett udda heltal större än 1.

1. Välj ett heltal a mellan 2 och $n - 1$.
2. Skriv $n - 1 = 2^k d$ där d är udda, dvs d är talet man får om man delar bort alla faktorer 2 från $n - 1$.
3. Testa om

$$\begin{aligned} a^d &\equiv \pm 1 \bmod n, \\ a^{2d} &\equiv -1 \bmod n, \\ a^{4d} &\equiv -1 \bmod n, \\ &\vdots \\ a^{2^k d} = a^{(n-1)/2} &\equiv -1 \bmod n. \end{aligned}$$

   Om ingen av kongruenserna gäller är n ett sammansatt tal.

Återigen, om vi kommer fram till att någon av kongruenserna är uppfyllda för något val av a så skulle n kunna vara ett primtal, men det är inte säkert. Exempelvis, om $n = 65 = 5 \cdot 13$ och $a = 18$ får vi $n - 1 = 2^6 \cdot 1$, i vilket fall

$$18^{2 \cdot 1} = 324 \equiv -1 \bmod 65,$$

så den andra kongruensen i steg 3 är uppfylld trots att 65 är ett sammansatt tal. Dock är situationen mycket bättre än för Fermats test, vilket visas av följande sats.

Sats. *Om n är ett sammansatt tal kommer Miller–Rabins test svara att n är sammansatt för åtminstone tre fjärdedelar av alla möjliga val för a.*

Som följd denna sats ser vi att om vi utför Miller–Rabins test med ett slumpmässigt valt a, så om n är sammansatt kommer testet svara att n är sammansatt med sannolikhet åtminstone 3/4. Detta kan upprepas. Om vi exempelvis utför Miller–Rabins test för 100 olika slumpmässigt valda värden på a, så om n är ett sammansatt tal kommer åtminstone något av testerna svara att n är sammansatt med sannolikhet åtminstone $1 - 1/4^{100} = 99{,}999999999999999999999999999999999999999999999999999999999999377\ldots\,\%$.