Gaussiska primtal

Christer Kiselman

Institut Mittag-Leffler & Uppsala universitet

1. Beskrivning av uppgiften. De förslag som presenteras här kan behandlas på flera olika sätt. Ett första syfte är helt enkelt att uppmärksamma att begreppet primtal inte är något absolut, utan beror på vad man relaterar det till. Man kan tänka sig en rent grafisk uppgift där det gäller att pricka in de gaussiska primtalen på ett papper för att åskådliggöra hur de fördelar sig i några olika områden. Om man vill gå längre kan man räkna ut tätheten inom några delar av det komplexa planet. En annan möjlighet är att skriva en uppsats som går igenom teorin för de gaussiska primtalen; då kan följande rader tjäna som ledning, och ett mål kan vara att i detalj visa allt som jag antyder eller uppmanar läsaren att visa. Ett mer avancerat projekt slutligen är att studera faktorisering i några andra ringar $\mathbf{Z}[\sqrt{d}]$ för heltal d; här handlar det ju bara om $d = -1$.

2. Vanliga primtal och komplexa primtal. Talen 2, 3, 5, 7, 11, ... är primtal, vilket betyder att man inte kan faktorisera dem utan att en faktor måste vara 1 eller -1. Vi kan till exempel skriva

$$19 = 1 \cdot 19 = 19 \cdot 1 = (-1) \cdot (-19) = (-19) \cdot (-1)$$

men inte på något annat sätt med heltal, medan däremot 21 kan faktoriseras som $3 \cdot 7$ eller $(-7) \cdot (-3)$. Man kan också räkna med komplexa tal $z = x+iy$ där x och y är vanliga heltal. Om vi betecknar de vanliga heltalen med $\mathbf{Z}$, så bildar alla tal av formen $z = x + iy$ med $x, y \in \mathbf{Z}$ en mängd $\mathbf{Z} + i\mathbf{Z}$ som också betecknas $\mathbf{Z}[i]$ och kallas *ringen av gaussiska heltal.* Dessa allmännare heltal är uppkallade efter Carl Friedrich Gauss (1777–1855).

I $\mathbf{Z}[i]$ inträffar nu att några av våra gamla primtal kan faktoriseras på ett nytt sätt. Vi kan t. ex. skriva

$$2 = (1+i)(1-i), \quad 5 = (2+i)(2-i) \quad \text{och} \quad 101 = (10+i)(10-i),$$

vilket visar att 2, 5 och 101, som är primtal i $\mathbf{Z}$, inte är primtal i $\mathbf{Z}[i]$. Begreppet primtal beror alltså på i vilken ring man räknar. Däremot förblir det gamla primtalet 3 ett primtal också i $\mathbf{Z}[i]$, ty det kan faktoriseras som

$$3 = 3 \cdot 1 = 1 \cdot 3 = i(-3i) = (-i)(3i)$$

och på några andra sätt med ± 1 eller $\pm i$ som faktor, men inte utan att en av dessa faktorer med absolutbelopp 1 uppträder. (Visa detta!) Nu kan ju alla gaussiska heltal faktoriseras som

$$z = 1 \cdot z = (-1)(-z) = i(-iz) = (-i)(iz),$$

så faktorer ± 1, $\pm i$ bör vi betrakta som oväsentliga, precis som ± 1 för de vanliga primtalen. Vi kan alltså nu definiera z som ett *gaussiskt primtal* om varje faktorisering $z = ab$ med $a, b \in \mathbf{Z}[i]$ måste ha endera $|a| = 1$ eller $|b| = 1$, dvs. en faktor måste vara i^k, $k = 0, 1, 2, 3$. Vi ser att dessa fyra element i $\mathbf{Z}[i]$ är de enda som har invers i $\mathbf{Z}[i]$, precis som ± 1 är de enda heltal som har invers i $\mathbf{Z}$.

Vi kan nu säga att ett tal i $\mathbf{Z}$ som inte är ett primtal inte heller kan vara primtal i $\mathbf{Z}[i]$, ty en faktorisering $z = ab$ med $a, b \in \mathbf{Z}$ gäller ju också i $\mathbf{Z}[i]$. Och som vi sett kan det inträffa att ett primtal i $\mathbf{Z}$ förblir primtal i den större ringen $\mathbf{Z}[i]$ (exempelvis talet 3) men också att det blir sammansatt i $\mathbf{Z}[i]$ (exempelvis $5 = (2+i)(2-i)$). Och dessutom finns det nya primtal i $\mathbf{Z}[i]$ som inte ligger i $\mathbf{Z}$ (exempelvis $1+i$; visa att det är ett gaussiskt primtal!).

3. Testa om ett gaussiskt heltal är prima. Skriv ett datorprogram som undersöker om ett givet tal $z \in \mathbf{Z}[i]$ är ett gaussiskt primtal eller ej. Om du har en dator som kan dividera komplexa tal direkt så är det bara att prova om z/c ligger i $\mathbf{Z}[i]$ för olika heltal $c \in \mathbf{Z}[i]$. Det räcker att testa med alla c som uppfyller $1 < |c| \leq \sqrt{|z|}$, dvs. ändligt många. Varför?

Om din dator inte kan dividera komplexa tal så får du låta den undersöka real- och imaginärdelarna för sig. Vi skriver kvoten z/c så här:

$$\frac{z}{c} = \frac{x+iy}{a+ib} = \frac{(a-ib)(x+iy)}{a^2+b^2} = \frac{ax+by+i(ay-bx)}{a^2+b^2}.$$

Tydligen är

$$\operatorname{Re}\frac{z}{c} = \frac{ax+by}{a^2+b^2} \qquad \text{och} \qquad \operatorname{Im}\frac{z}{c} = \frac{ay-bx}{a^2+b^2},$$

och z/c är ett gaussiskt heltal precis när både $\operatorname{Re}(z/c)$ och $\operatorname{Im}(z/c)$ är vanliga heltal. Som sagt, det räcker att undersöka detta för $c = a+ib$ med $1 < |c|^2 = a^2+b^2 \leq |z|$. Det räcker till och med att kontrollera sådana c som ligger i den första kvadranten, dvs. sådana som uppfyller $a \geq 0$ och $b \geq 0$. Varför? Dessa anmärkningar kan spara tid om datorn inte är så snabb.

Gör ett program som trycker ut alla gaussiska primtal upp till en viss gräns. Pricka sedan in dem i ett diagram — eller låt datorn göra det. Under sökandet behöver man bara undersöka en åttondel av planet, t. ex. $z = x+iy$ med $0 \leq y \leq x$, ty talen $\pm z$, $\pm\bar{z}$, $\pm iz$, $\pm i\bar{z}$ är primtal samtidigt, och ett av dem ligger i oktanten $0 \leq y \leq x$. Vilka tal är det som är primtal i $\mathbf{Z}$ men upphör att vara det i $\mathbf{Z}[i]$? Går det att säga något om hur de gaussiska primtalen fördelar sig i det komplexa talplanet? Kan du se om de ligger tätare kring origo än långt från origo? (Troligen måste man ha ett ganska stort diagram för att kunna se det.)

4. Samband mellan de olika typerna av primtal. Om $z = x + iy$ är ett gaussiskt heltal så beskaffat att $|z|^2 = x^2 + y^2$ är ett primtal i $\mathbf{Z}$, så är z ett primtal i $\mathbf{Z}[i]$. Visa det! Med detta kriterium kan vi till exempel se att $10 + 3i$ är prima, ty dess absolutbelopp i kvadrat är $|10+3i|^2 = 10^2+3^2 = 109$ som är ett primtal i $\mathbf{Z}$. Omvänt kan vi fråga oss om $|z|^2$ är ett primtal i $\mathbf{Z}$ om z är ett primtal i $\mathbf{Z}[i]$. Svaret är nej, ty 3 är ett gaussiskt primtal medan $|3|^2 = 9$ inte är prima. Men om vi tar ett primtal $z = x + iy$ med realdel $x \neq 0$ och imaginärdel $y \neq 0$, är då $|z|^2 = x^2 + y^2$ ett vanligt primtal? Försök visa att det är så! (Ledning: använd att $\mathbf{Z}[i]$ har unik faktorisering; en faktorisering av $z\bar{z} = ab$ leder till en faktorisering

$$z = \frac{a}{\bar{z}} \cdot b = a \cdot \frac{b}{\bar{z}}$$

av z, där $a/\bar{z}$ eller $b/\bar{z}$ är ett gaussiskt heltal.)

Vi kan dela in de vanliga positiva primtalen i tre klasser efter vilken rest de ger vid division med fyra: 5, 13, 17, ... som ger resten 1 vid division med fyra; 3, 7, 11, 19, ... som ger resten 3; och så det återstående primtalet som är 2, det enda jämna primtalet. Det visar sig nu att inget primtal i den första klassen, alltså de som har formen $4k + 1$ för något heltal k, är primtal i $\mathbf{Z}[i]$. De kan alla faktoriseras som $p = (a + ib)(a - ib)$. Man kan nämligen visa att ett sådant primtal p kan skrivas $p = a^2 + b^2$ för några tal a och b; ett bevis för detta finns i till exempel LeVeque [1956, volym I, kapitel 7]. Talen $a + ib$ och $a - ib$ måste vara gaussiska primtal. (Vad är nämligen kvadraten på deras absolutbelopp?)

De positiva primtalen av typen $p = 4k+3$ däremot är primtal även i den större ringen $\mathbf{Z}[i]$. Försök visa detta! Kanske kan följande vara till hjälp: om p kunde faktoriseras i $\mathbf{Z}[i]$, $p = (a + ib)(c + id)$, så skulle

$$p^2 = |p|^2 = |a + ib|^2|c + id|^2 = (a^2 + b^2)(c^2 + d^2).$$

Och om $|a+ib| > 1$ och $|c+id| > 1$ så måste $p = a^2 + b^2$. Vilka rester kan nu ett tal av formen $a^2 + b^2$ ge vid division med 4?

Talet 2, slutligen, som är primtal i $\mathbf{Z}$, är som vi redan sett inte primtal i $\mathbf{Z}[i]$.

5. Fördelning av primtalen. Om fördelningen av de gaussiska primtalen kan vi säga något intressant när vi vet något om fördelningen av de positiva primtalen. Det resultat som uttalar sig om denna kallas primtalssatsen och bevisades år 1896 av Jacques Hadamard och Charles de La Vallée-Poussin. Primtalssatsen säger att antalet primtal p med $2 \leq p \leq x$, betecknat $\pi(x)$, uppfyller en asymptotisk relation

$$\pi(x) \sim \frac{x}{\log x},$$

där tecknet $\sim$ betyder att kvoten mellan de bägge leden går mot 1 då $x \to +\infty$, dvs.

$$\pi(x) = \frac{x}{\log x}\,(1 + g(x))$$

där $g(x) \to 0$ då $x \to +\infty$. Läs något mer om primtalssatsen i till exempel Carleson [1968], Hardy & Wright [1979], Newman [1980] eller Riesel [1968; 1985].

Vi delar in π i tre delar, svarande mot resterna vid division med 4,

$$\pi = \pi_1 + \pi_2 + \pi_3,$$

där π_1 räknar primtalen av typ $4k+1$, π_2 det enda jämna primtalet (alltså $\pi_2(x) = 1$ om $x \geq 2$, $\pi_2(x) = 0$ annars), och π_3 räknar primtalen av typ $4k+3$.

Till primtalen av typ $4k+1$ hör åtta gaussiska primtal, nämligen $\pm a \pm ib$ och $\pm b \pm ia$, alla med absolutbelopp $\sqrt{p}$. Det blir verkligen

åtta olika tal, ty $a \neq 0$, $b \neq 0$ och $a \neq b$. Antalet gaussiska primtal z med $|z| \leq r$ som vi får fram genom att ta $p = 4k + 1$ blir alltså $8\pi_1(r^2)$.

Till primtalet 2 hör de fyra gaussiska primtalen $\pm 1 \pm i$. Antalet gaussiska primtal z av denna typ är alltså $4\pi_2(r^2)$.

Till primtalen $p = 4k + 3$ hör fyra gaussiska primtal $z = i^m p$, $m = 0, 1, 2, 3$. De har alla samma absolutbelopp som p, varav följer att de som uppfyller $|z| \leq r$ är $4\pi_3(r)$ till antalet.

När vi räknar ihop alla gaussiska primtal z i cirkelskivan $|z| \leq r$ blir deras antal således

$$\gamma(r) = 8\pi_1(r^2) + 4\pi_2(r^2) + 4\pi_3(r).$$

Denna formel gäller exakt, men för att få reda på hur antalet växer med r måste vi veta något om hur stora π_1 och π_3 är jämfört med varandra. Det är nu känt att det är ungefär lika vanligt att ett primtal är av typen $4k + 1$ som av typen $4k + 3$, dvs.

$$\pi_1(x) \sim \frac{x}{2\log x} \qquad \text{och} \qquad \pi_3(x) \sim \frac{x}{2\log x}.$$

Eftersom $\pi_2(x) \sim 1$ så får vi

$$\gamma(r) \sim 8\frac{r^2}{2\log r^2} + 4 + 4\frac{r}{2\log r} = \frac{2r^2}{\log r} + 4 + \frac{2r}{\log r} \sim \frac{2r^2}{\log r}.$$

Vi ser att de gaussiska primtal som ligger utanför de två axlarna och har absolutbelopp $> \sqrt{2}$ (dvs. de som räknas av den första termen) överväger.

Medeltätheten av de gaussiska primtalen i cirkelskivan $|z| \leq r$ blir $\gamma(r)$ dividerat med skivans area:

$$\frac{\gamma(r)}{\pi r^2} \sim \frac{2}{\pi \log r}.$$

Vi kan nu jämföra denna med medeltätheten i intervallet $[-x, x]$ av de vanliga primtalen, som är

$$\frac{2\pi(x)}{2x} \sim \frac{1}{\log x}.$$

Vi kan uttrycka dessa resultat så här: sannolikheten att ett vanligt heltal x med stort absolutbelopp skall vara ett primtal i $\mathbf{Z}$ är $\sim 1/\log|x|$, medan sannolikheten att ett gaussiskt heltal z med stort absolutbelopp skall vara ett primtal i $\mathbf{Z}[i]$ är $\sim 2/\pi \log|z|$. (Sannolikheten i ett visst område $\{z; |z-a| \leq r\}$ blir ungefär lika med sannolikheten i hela skivan $\{z; |z| \leq |a|\}$ om $|a|$ är stort jämfört med r.)

Låt datorn räkna ut $\gamma(r)$ och $\pi(x)$ för några värden på r och x och se hur det stämmer.

En bättre approximation än $\pi(x) \sim x/\log x$ är den som Legendre fann 1808:

$$\pi(x) \sim \frac{x}{\log x - 1,08366}.$$

Man kan därför bestämma $a(r)$ så att

$$\gamma(r) = \frac{2r^2}{\log r - a(r)}.$$

Då bör $a(r)$ få ett värde som inte varierar så mycket.

Litteratur

Carleson, L., *Matematik för vår tid.* Prisma, Stockholm 1968.

Hardy, G. H. & Wright, E. M., *An introduction to the theory of numbers.* Fifth edition, Oxford Univ. Press, Oxford 1979.

LeVeque, W. J., *Topics in Number Theory, I & II.* Addison-Wesley 1956.

Newman, D. J., Simple analytic proof of the prime number theorem. *Amer. Math. Monthly* 87 (1980), s 693–696.

Riesel, H., *En bok om primtal.* Studentlitteratur 1968. Odense 1968.

Boken är slutsåld från förlaget, men författaren har några exemplar kvar.

Riesel, H., *Prime Numbers and Computer Methods for Factorization.* Birkhäuser 1985.