MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Samuel Lundqvist
14 December 2013

Ekvationer över ändliga kroppar

Det här texten handlar främst om polynomekvationer i $\mathbb{Z}_p$, där p är ett primtal, men även om polynomekvationer i $\mathbb{Z}_m$.
Vi kommer att använda

- Faktorsatsen (Sats 22.8.1 i Biggs), som endast håller i kroppar. Faktorsatsen lyder "Ekvationen $f(x) = 0$ har en rot $x = a$ om och endast om $x - a$ är en faktor[1] till $f(x)$, dvs $f(x) = (x - a)q(x)$.Följdsatsen 22.8.2, att en polynomekvation av grad n har högst n lösningar, är viktigt. Faktorsatsen gäller för godtyckliga kroppar, men om vi arbetar i $\mathbb{Z}_p$ där p är mindre än n så finns det så klart högst p olika lösningar till en ekvation av grad n.
- Eulers sats, att $x^{\phi(m)} = 1$ för alla $x \neq 0$ i $\mathbb{Z}_m$.

Linjära ekvationer på formen $ax + b = 0$ $(a \neq 0)$ i $\mathbb{Z}_p$

En linjär ekvation löser vi som vanligt genom $ax + b = 0 \Leftrightarrow ax = -b \Leftrightarrow x = -a^{-1}b$.

Exempel 1. *$5x + 1 = 0$ i $\mathbb{Z}_7$ löser vi genom $5x + 1 = 0 \Leftrightarrow 5x = 6 \Leftrightarrow x = 3 \cdot 6 = 4$, eftersom 6 är den additiva inversen till 1 och 3 är den multiplikativa inversen till 5.*

Om p är ett litet primtal kan man också göra en totalsökning. För varje $c \in \mathbb{Z}_p$ testar vi om $ac + b = 0$. När vi hittat ett c är vi klara, eftersom det finns precis en lösning.

Andragradsekvationer på formen $ax^2 + bx + c = 0$ $(a \neq 0)$ i $\mathbb{Z}_p$

Först och främst är det inte säkert att det finns lösningar till en andragradsekvation. Ett klassiskt exempel är ekvationen $x^2 + x + 1 = 0$ i $\mathbb{Z}_2[x]$. Genom insättning ser man att varken $x = 0$ eller $x = 1$ satisfierar ekvationen. Polynomet $x^2 + x + 1$ är alltså ett exempel på ett *irreducibelt* polynom (för den teorin hänvisas till Biggs, speciellt sid 311-312). När kroppen är liten är insättning den mest användbara metoden. (Men det går även att kvadratkomplettera på samma sätt som man är van vid när det gäller andragradsekvationer över de reella talen.)
Låt $f(x) = ax^2 + bx + c$. När man hittat en lösning x_1 till ekvationen $f(x) = 0$ så följer det av faktorsatsen att $x - x_1$ är en faktor till $f(x)$. Alltså kan vi skriva $f(x) = (x - x_1) \cdot q(x)$, där $q(x)$ är ett linjärt polynom som har precis en lösning, som vi kallar x_2. Vi har $f(x_2) = (x - x_1) \cdot q(x_2) = (x_2 - x_1) \cdot 0 = 0$, så $x = x_2$ är en lösning även till $f(x) = 0$.
Man kan även välja att göra totalsökning för att fram den andra roten.

Exempel 2. *Låt $f(x) = x^2 + 2 \in \mathbb{Z}_3[x]$. Genom insättning finner vi att $x = 1$ en lösning till $f(x) = 0$. Alltså är $x + 2$ en faktor. Genom polynomdivision får vi $f(x) = (x + 2)(x + 1)$ och det är nu lätt att läsa av att $x = 2$ är en annan lösning, eftersom $x = 2$ är en rot till ekvationen $x + 1 = 0$.*

Exempel 3. *Låt $f(x) = x^2 + 2x + 1 \in \mathbb{Z}_3[x]$. Går man igenom alla tre element i $\mathbb{Z}_3$ ser man det endast $x = 2$ är en lösning. Det kan man även se genom att utföra polynomdivision med $x + 1$ och få $f(x) = (x + 1)(x + 1)$. Lösningen $x = 2$ är alltså en dubbelrot.*

[1] Om man ska vara noga bör man påpeka att $x - a$ avses uttrycket $x + (-a)$

Högre ekvationer

Ekvationer av högre grad än två kan behandlas på precis samma sätt som andragradsekvationer - genom upprepad insättning och polynomdivision, alternativt endast genom insättning. Detta är emellertid inte effektivt om kroppen har många element, om det är många termer inblandade eller om graden på polynomet är stort. Då behövs effektivare metoder.

Högre ekvationer på formen $x^n = a$, $a \neq 0$

Vi löser det här problemet i ett specialfall. Antag att n och $p-1$ är relativt prima. I detta fall finns det s, t så att $sn + t(p-1) = 1$ i $\mathbb{Z}$. Det gäller att $x^n = a \Rightarrow (x^n)^s = a^s \Leftrightarrow x^{ns} = a^s \Leftrightarrow x^{1-t(p-1)} = a^s \Leftrightarrow x^1 \cdot (x^{p-1})^{-t} = x \cdot 1^{-t} = a^s \Leftrightarrow x = a^s$ där vi har utnyttjat Eulers sats/Fermats lilla sats, eftersom vi kan utgå från att x är nollskild (då $a \neq 0$).
Så vi har en implikation $x^n = a \Rightarrow x = a^s$ i $\mathbb{Z}_p$, där s är den muliplikatva inversen till n i $\mathbb{Z}_{p-1}$ (som existerar på grund av antagandet att n och p-1 är relativt prima).
Men vi kan gå åt andra hållet också. Vi har att $x = a^s \Rightarrow x^n = (a^s)^n = a^{sn} = a^{t(p-1)+1} = a^{t(p-1)+1} = (a^{p-1})^t \cdot a = 1^t \cdot a = a$.
Det gäller alltså $x^n = a \Leftrightarrow x = a^s$ och det innebär att ekvationen $x^n = a$ har exakt en lösning $x = a^s$ i $\mathbb{Z}_p$ om n och $p-1$ är relativt prima.

Exempel 4. *Ekvationen $x^5 = 3$ i $\mathbb{Z}_7$ har en unik lösning, ty 5 och $7-1 = 6$ är relativt prima. För att finna den använder vi Euklides algoritm för att få likheten $1 = 5 \cdot 5 + 6 \cdot (-4)$ och det följer nu att $x^5 = 3 \Leftrightarrow x = 3^5 = 5$.*

Notera att vi gjort liknande räkningar i teorin för RSA, men där arbetar vi i $\mathbb{Z}_m$, där $m = p_1 \cdot p_2$, en produkt av två primtal. Det gäller faktiskt mer allmänt att $x^n = a$ har unik lösning i $\mathbb{Z}_m$ om n och $\phi(m)$ är relativt prima. Denna lösning är $x = a^s$, där s är den multiplikativa inversen till n i $Z_{\phi(m)}$ och beviset är på precis samma sätt som ovan. Det lämnas som övning till läsaren att verifiera detta.

Exempel 5. *Ekvationen $x^5 = 3$ i $\mathbb{Z}_6$ har en unik lösning, ty 5 och $\phi(6) = 2$ är relativt prima. För att finna den använder vi Euklides algoritm för att få likheten $1 = 5 \cdot 1 - 2 \cdot 2$,vilket innebär att 1 är den multipliaktiva inversen till 5 i $\mathbb{Z}_{\phi(m)} = \mathbb{Z}_2$, och det följer nu att $x^5 = 3 \Leftrightarrow x = 3^1 = 3$. I detta fall kan man även använda den direkta metoden att skriva om $x^5 = x^2 \cdot x^2 \cdot x$ och sedan utnyttja att $x^2 = 1$ i $\mathbb{Z}_6$ (Eulers sats), vilket ger att $x^5 = x$, och ekvationen förenklas alltså till $x = 3$.*

När n och $p-1$ inte är relativt prima får man olika utslag. Vi har t.ex. att ekvationen $x^{p-1} = 1$ har exakt $p-1$ lösningar i $\mathbb{Z}_p$, nämligen $x = 1, \ldots, p-1$, medan ekvationen $x^{p-1} = 2$ helt saknar lösningar.

Andra typer av ekvationer

Linjära ekvationssystem i flera variabler över kroppar kan behandlas med Gausselimination precis som vi är vana vi, vilket vi ska se i teorin för felrättande koder. System av polynomekvationer av högre grad än ett i flera variabler över ändliga kroppar kan lösas genom insättning (återigen, om kroppen är tillräckligt liten, annars behövs mer sofistikerade metoder). Ekvationer över ändliga ringar, t.ex. Z_m där m inte är ett primtal kan också lösas genom insättning. Men här gäller inte faktorsatsen.

Exempel 6. *För att finna alla lösningar till systemet $x^2 + y^2 = 0, x^3 + 2y^3 = 0$ över $\mathbb{Z}_5$ kan vi gå igenom alla 25 par $(a, b), a, b \in \mathbb{Z}_5$. En liten genväg är att sätta $x = 0$ och notera att detta medför att $y = 0$, sedan sätta $x = 1$, osv.*