Het orde–lemma

Christophe Debry

Zij G een eindige commutatieve groep, met eenheidselement 1 en multiplicatief genoteerd. De orde van een element $g \in G$ is het kleinste natuurlijk getal $n \in \mathbb{N}_0$ waarvoor geldt dat $g^n = 1$.

> De orde van 2 in de groep $\mathbb{Z}_7^\times, \cdot$ is gelijk aan 3. Inderdaad, $2^1 \equiv 2 \mod 7$, $2^2 \equiv 4 \mod 7$, $2^3 \equiv 1 \mod 7$. In $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ heeft elk element (dat niet het eenheidselement is) orde 2. Een eindige commutatieve groep G is cyclisch als en slechts als er een element van G bestaat met orde $|G|$.

Orde–lemma

Zij G een eindige commutatieve groep, $g \in G$ en n de orde van g. Voor alle $x, y \in \mathbb{Z}$ geldt er dat $g^x = g^y$ als en slechts als $x - y$ deelbaar is door n. In het bijzonder geldt $g^x = 1$ als en slechts als x deelbaar is door n.

> Het is voldoende de bijzondere uitspraak te bewijzen. De "als"–implicatie is evident, dus stel omgekeerd dat $g^x = 1$. Het delingsalgoritme levert een $q \in \mathbb{Z}$ en een $r \in \{0, 1, \ldots, n-1\}$ met $x = qn + r$. Hiervoor geldt dat $1 = g^x = (g^n)^q \cdot g^r = g^r$. Maar n is het kleinste niet–nul natuurlijk getal met $g^n = 1$, dus volgt uit $0 \leq r < n$ dat $r = 0$. We vinden dat $x = qn + r = qn$ deelbaar is door n. ■

De deelgroep van G voortgebracht door g heeft orde n (waarom?), en dus vertelt de stelling van Lagrange voor groepen ons dat n een deler is van $|G|$. Het lemma impliceert nu dat $g^{|G|} = 1$ voor alle $g \in G$, maar vooral het feit dat de orde van element steeds de orde van de groep deelt, is de moeite waard om te onthouden. Als speciaal geval van de gelijkheid $g^{|G|} = 1$ vinden we voor $G = \mathbb{Z}_n^\times, \cdot$ dat $[a]_n^{\varphi(n)} = 1$, i.e., dat $a^{\varphi(n)} \equiv 1 \mod n$ voor alle gehele getallen a die onderling ondeelbaar zijn met n. Voor n priem is dit precies de kleine stelling van Fermat.

Als $a \in \mathbb{Z}$ en $n \in \mathbb{N}_0$, dan noemen we de orde van $[a]_n$ in $\mathbb{Z}_n^\times, \cdot$ kortweg *de orde van a modulo n*. Merk op dat deze orde sowieso $\varphi(n)$ deelt omwille van bovenstaande opmerkingen.

> Om na te gaan dat de orde van 2 modulo 7 gelijk is aan 3, is het voldoende na te gaan dat $2 \not\equiv 1 \mod 7$ en dat $2^3 \equiv 1 \mod 7$ omdat de orde dan niet 1 kan zijn (omwille van de eerste niet–congruentie), en niet 2 omdat uit de tweede congruentie volgt dat de orde een deler is van 3. Als $g \in G$ en $k \in \mathbb{N}$ met $g^{2^k} = -1$ (i.e., een element van G met orde 2), dan is de orde van g gelijk aan 2^{k+1}. Als $a, n \in \mathbb{N} \setminus \{0, 1\}$, dan is $\varphi(a^n - 1)$ deelbaar door n. Inderdaad, in $\mathbb{Z}_{a^n-1}^\times$ geldt dat $a^{\varphi(a^n-1)} = 1$, en de orde van a in deze groep is duidelijk gelijk aan n.

Gevolg 1

Zij $n \in \mathbb{N} \setminus \{0, 1\}$. Stel dat a en b gehele getallen zijn die onderling ondeelbaar zijn met n en zodat $a^n - b^n$ deelbaar is door n. Dan is $a - b$ deelbaar door de kleinste priemdeler van n.

Zij p de kleinste priemdeler van n. Omdat a en b onderling ondeelbaar zijn met n, bestaat de inverse c van a in $\mathbb{Z}_n^\times$. Er is gegeven dat $(bc)^n - 1$ deelbaar is door n en dus ook door p. De orde van bc in $\mathbb{Z}_p^\times$ deelt dus zowel n als $\varphi(p) = p - 1$, en aangezien n geen kleinere priemdelers dan p heeft, moet deze orde 1 zijn. Bijgevolg is $bc \equiv 1 \mod p$, en dus $a \equiv b \mod p$. ■

Als toepassing bewijzen we dat als $n \in \mathbb{N} \setminus \{0, 1\}$ en $3^n + 4^n$ deelbaar is door n, dan is n deelbaar door 7. Inderdaad, n is duidelijk niet deelbaar door 2 of 3, dus n is oneven. Bijgevolg is $3^n - (-4)^n$ deelbaar door n, waarbij 3 en -4 onderling ondeelbaar zijn met n. Het lemma vertelt ons dat $3 + 4 = 7$ deelbaar is door de kleinste priemdeler van n, en dus is deze kleinste priemdeler gelijk aan 7.

Gevolg 2

Zij p een priemgetal. Dan bestaat er een priemgetal q zodat $q - 1$ deelbaar is door p.

Neem voor q een priemdeler van $2^p - 1$. Dan is $q \neq 2$ en dus deelt de orde d van 2 modulo q zowel p als $q - 1$. Omdat p priem is, moet $d = 1$ of $d = p$. Het eerste is onmogelijk, en dus moet $p = d$ een deler zijn van $q - 1$. ■

Een eenvoudig gevolg is dat er oneindig veel priemgetallen zijn: als er maar eindig veel waren, neem dan voor p het grootste priemgetal, dan bestaat er een priemgetal q met $q-1$ deelbaar door p en dus $q > q - 1 \geq p$, contradictie. Een ander gevolg is de oplossing van het inverse Galoisprobleem voor $\mathbb{Z}_p$.[1] Inderdaad, neem q uit het lemma. Het veld $L = \mathbb{Q}\left(e^{2\pi i/q}\right)$ heeft Galois–groep $\mathbb{Z}_q^\times$ over $\mathbb{Q}$, en deze heeft orde $q - 1$. Omdat p hier een deler van is, bestaat er volgens Sylow/Cauchy een element van orde p in $\mathbb{Z}_q^\times$, i.e., $\mathrm{Gal}(L/\mathbb{Q})$ heeft een deelgroep H van orde p. Neem nu voor K het vasteveld van L onder de actie van H, want dan is $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = |H| = p$, waaruit $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p$ volgt.

Gevolg 3

Zij p een priemgetal en $x \neq 1$ een natuurlijk getal. Stel dat q een priemdeler is van

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1.$$

Dan is $q = p$ of $q \equiv 1 \mod p$.

[1] Het inverse Galoisprobleem voor een eindige groep G: bestaat er een eindige Galois–uitbreiding K van $\mathbb{Q}$ zodat $\mathrm{Gal}(K/\mathbb{Q}) \cong G$? In het algemeen weet men nog niet wat het antwoord is, maar het is wel affirmatief beantwoord voor oplosbare (en dus zeker voor commutatieve) groepen.

We weten dat $x^p \equiv 1 \mod q$, dus q en x zijn onderling ondeelbaar. Zij d de orde van x modulo q. Dan is d een deler van p volgens het gegeven en een deler van $q-1$ volgens de kleine stelling van Fermat. Er geldt dus dat $d = 1$ of $p|q-1$. In het tweede geval zijn we klaar. Als $d = 1$, dan is $x \equiv 1 \mod q$, dus moet

$$0 \equiv \frac{x^p - 1}{x - 1} \equiv x^{p-1} + x^{p-2} + \ldots + x + 1 \equiv 1 + 1 + \ldots + 1 \equiv p \mod q,$$

zodat $p = q$ aangezien p en q priemgetallen zijn. ■

Als rechtstreekse toepassing volgt er dat als p priem is, dan heeft $p^p - 1$ een priemdeler die congruent is met 1 modulo p. Inderdaad, neem een priemdeler q van $(p^p - 1)/(p-1)$. Het is duidelijk dat $q \neq p$, en dus volgt er dat $q \equiv 1 \mod p$.

Opgaven

1 *Opwarmers: oefen de definitie in*

(a) Bewijs dat een oneven priemdeler van een getal van de vorm $n^2 + 1$ steeds congruent is met 1 modulo 4. Een priemdeler van een getal van de vorm $n^4 - n^2 + 1$ is congruent met 1 modulo 12.
(Wat is de orde van n modulo zo'n priemdeler?)

(b) Toon aan dat elke priemdeler van een Fermat–getal $2^{2^n} + 1$ congruent is met 1 modulo 2^{n+1}.
(Wat is de orde van 2 modulo zo'n priemdeler?)

(c) Zij p een oneven priemgetal met $p \equiv 2 \mod 3$. Bewijs dat de afbeelding $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto x^3$ injectief is. Besluit (zoals gevraagd op Balkan 1999) dat er hoogstens p getallen in

$$S = \left\{ y^2 - x^3 - 1 \mid x, y \in \{0, 1, \ldots, p-1\} \right\}$$

zitten die deelbaar zijn door p.

2 *Opwarmers: oefen gevolg 1 in*

(a) (Putnam 1939) Vind alle $n \in \mathbb{N}$ zodat $2^n - 1$ deelbaar is door n.

(b) (Baltic Way 2006) Vind alle $n \in \mathbb{N}_0$ zodat $3^n + 1$ deelbaar is door n^2.

3 (LIMO 2007, Baltic Way 2005, Arne Smeets) Zij n een natuurlijk getal, zij p een priemgetal en zij d een deler van $(n+1)^p - n^p$. Bewijs dat $d - 1$ deelbaar is door p.

4 Vind alle priemgetallen p en q zodat $(5^p - 2^p)(5^q - 2^q)$ deelbaar is door pq.

5 *Machten van 2*

(a) Vind alle priemgetallen p en q zodat $2^p + 2^q$ deelbaar is door pq.

(b) Vind alle natuurlijke getallen n zodat $2^{n-1} + 1$ deelbaar is door n.

6 (LIMO 2008, Hendrik W. Lenstra) Bestaat er een strikt positief geheel getal n dat deelbaar is door 103 en zodat $2^{2n+1} \equiv 2 \mod n$?

7 (2003 USA IMO TST) Vind alle drietallen (p, q, r) van priemgetallen waarvoor geldt dat

$$p|q^r + 1,\ q|r^p + 1,\ r|p^q + 1.$$

8 (IMC 2011) Zij p een priemgetal. We noemen een natuurlijk getal n (niet nul) p–interessant als er veeltermen $f(X), g(X) \in \mathbb{Z}[X]$ bestaan met

$$X^n - 1 = (X^p - X + 1)f(X) + pg(X).$$

Toon voor elk priemgetal p aan dat $p^p - 1$ een p–interessant getal is.

9 (IMOSL 2006, N6) Bepaal alle gehele getallen x en y waarvoor geldt dat

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

10 (IMOSL 2003/6) Zij p een priemgetal. Bewijs dat er een priemgetal q bestaat dat voor geen enkel geheel getal n een deler is van $n^p - p$.

Hints

3 Zij q een priemdeler van d. De orde van $(n + 1) \cdot n^{-1}$ modulo q is een deler van p.

4 p deelt $5^p - 2^p$ of $5^q - 2^q$. Als $p \neq 3$ dan zegt Gevolg 1 dat het eerste geval onmogelijk is en dus dat $q \mid p - 1$.

5 De "machten van 2" titel is zelf een hint. (Beschouw $\min(p, q) = 2$ apart.) In de oplossing van (a) zal je $p - 1$ moeten schrijven als $2^\alpha a$, waarbij a oneven is, en analoog voor $q - 1 = 2^\beta b$. De orde van 2^a modulo q is gelijk aan $2^{\alpha+1}$.

6 De orde van 4 modulo 103 is deelbaar door 17, dus n is deelbaar door 17.

7 Beschouw het geval $\min(p, q, r) = 2$ apart. Als $p, q, r \geq 3$ dan is de orde van q modulo p gelijk aan 2 of $2r$. Bijgevolg is $p \mid q + 1$ of $2r \mid p - 1$.

8 Toon aan dat $K := \mathbb{F}_p[X]/(X^p - X + 1)$ een veld is. Dus $X^{p^p-1} = 1$ in K, omdat $K^\times$ een groep is van orde $p^p - 1$.

9 Gevolg 3 impliceert dat $y - 1$ en $y^4 + y^3 + y^2 + y + 1$ beiden congruent zijn met 0 of 1 modulo 7.

10 Zij d een priemdeler van $(p^p - 1)/(p - 1)$. Als d een deler is van een $n^p - p$, dan is de orde van n modulo d gelijk aan p^2.