Matematik, KTH
B.Ek

SF1662, Diskret matematik för CLGYM1, TSVDK2, CELTE2
vt 2015

Svar till övning 10, den 24 april 2015

1. $|G| = |G_x| \cdot |Gx|$ om G verkar på en mängd X, där $x \in X$.
Då x är ett hörn fås $|G_x| = 4$ (fyra rotationer kring en axel genom oktaederns mittpunkt och hörnet) och $|Gx| = 6$ (hörnet kan rotera till alla oktaederns hörn).
Om x är mittpunkten av en sidoyta fås på liknande sätt $|G_x| = 3$, $|Gx| = 8$.
I båda fallen blir $|G| = 24$.

2. Vi använder Burnsides lemma.
Brickans grupp av symmetrirotationer har i a. 8 element (kvadratens symmetrigrupp; $|G_x| = 2$, $|Gx| = 4$ för alla hörn x): identitetselementet (bevarar alla konfigurationer, $|X_{id}| = 3^4$), två rotationer $\pm\frac{\pi}{2}$ kring axeln vinkelrätt mot brickan genom dess mittpunkt (bevarar konfigurationer med samma färg på alla kulor, $|X_g| = 3$), en rotation π kring samma axel (bevarar alla konfigurationer med kulorna parvis likfärgade, $|X_g| = 3^2$), två rotationer π kring diagonalerna (bevarar konfigurationer med samma färg på två av kulorna, $|X_g| = 3^3$) och två rotationer π kring axlar genom mittpunkten och parallella med två kanter (bevarar konfigurationer med kulorna parvis likfärgade, $|X_g| = 3^2$). I b. är det bara 4 element i symmetrigruppen (de som inte vänder brickan).
Lemmat ger antalet väsentligt olika färgningar, $\frac{1}{|G|}\sum_{g\in G}|X_g|$, dvs i a. $\frac{1}{8}(3^4+2\cdot 3+3^2+2\cdot 3^3+2\cdot 3^2) = \frac{1}{8}3(27+2+3+18+6) = 21$ och i b. $\frac{1}{4}(3^4+2\cdot 3+3^2) = \frac{1}{4}3(27+2+3) = 24$. Svaren i c. fås genom att byta 3 mot k i a. och b., $\boldsymbol{\frac{1}{8}(k^4+2k^3+3k^2+2k)}$ och $\boldsymbol{\frac{1}{4}(k^4+k^2+2k)}$.

3. Burnsides lemma. (Den regelbundna) tetraederns grupp av symmetrirotationer har 12 element: Identitetselementet (bevarar alla konfigurationer, $|X_{id}| = k^6$), åtta rotationer $\pm\frac{2\pi}{3}$ kring axlar genom ett hörn och mittpunkten av motstående sidoyta (bevarar konfigurationer med samma färg på kanterna vid hörnet och samma på kanterna vid sidoytan, $|X_g| = k^2$) och tre rotationer π kring axlar genom mittpunkterna av motstående kanter (bevarar konfigurationer med övriga fyra kanter parvis likfärgade, $|X_g| = k^4$).
Lemmat ger antalet väsentligt olika färgningar, $\boldsymbol{\frac{1}{12}(k^6+3k^4+8k^2)}$.

4. RSA med $n = 77 = 7\cdot 11$, så $m = (7-1)(11-1) = 60$.
a. $\text{sgd}(45, m) = 15 \neq 1$, så 45 duger inte som e.
b. Euklides algoritm ger $1 = -8\cdot 60 + 37\cdot 13$, så $d = 37$.
c. 3 krypteras som $E(3) \equiv 3^{13} \pmod{77}$. Man finner $(3^2 = 9, 3^4 = 81 \equiv 4, 3^8 \equiv 16)$ $3^{13} = 3^8\cdot 3^4\cdot 3 \equiv 16\cdot 4\cdot 3 \equiv 38 \pmod{77}$, så 3 krypteras som 38.
d. 2 avkrypteras som $D(2) \equiv 2^{37} \pmod{77}$. Man finner $D(2) = 51$.

5. RSA med $n = 265 = 5\cdot 53$, så $m = (5-1)(53-1) = 208$. $e = 37$ och Euklides algoritm ger $1 = -8\cdot 208 + 45\cdot 37$, så $d = 45$. Meddelandet 2 avkrypteras alltså som $D(2) \equiv 2^{45} \equiv 147 \pmod{265}$, så som 147.

6. $E(x) \equiv 718^e = 718^{143} \pmod{1333}$ och $e = 143 = (10001111)_2$.
$x^2 = 718^2 = 515524 \equiv 986 \pmod{1333}$, $x^4 = 986^2 = 972196 \equiv 439 \pmod{1333}$ etc. ger $E(x) \equiv x^{128} \cdot x^8 \cdot x^4 \cdot x^2 \cdot x \equiv 986 \cdot 769 \cdot 439 \cdot 986 \cdot 718 \equiv 707 \pmod{1333}$, så $E(718) = 707$.
Alternativt kan man räkna så (eftersom $143 = (10001111)_2$):
$E(x) \equiv (((((((1^2 \cdot \underset{1}{x})^2 \cdot \underset{0}{1})^2 \cdot \underset{0}{1})^2 \cdot \underset{0}{1})^2 \cdot \underset{1}{x})^2 \cdot \underset{1}{x})^2 \cdot \underset{1}{x})^2 \cdot \underset{1}{x} \pmod{1333}$.
P.s.s. fås $E(719) \equiv (((((((1^2 \cdot 719)^2 \cdot 1)^2 \cdot 1)^2 \cdot 1)^2 \cdot 719)^2 \cdot 719)^2 \cdot 719)^2 \cdot 719 \equiv \cdots \equiv 615 \pmod{1333}$ och $E(719) = 615$.
$n = 1333 = 31 \cdot 43$ ger $m = 30 \cdot 42 = 1260$.
Euklides algoritm: $1260 = 8 \cdot 143 + 116$, $143 = 1 \cdot 116 + 27$, $116 = 4 \cdot 27 + 8$, $27 = 3 \cdot 8 + 3$, $8 = 2 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, så $1 = 3 - 2 = 3 - (8 - 2 \cdot 3) = -8 + 3 \cdot 3 = \cdots = -53 \cdot 1260 + 467 \cdot 143$, så vi tar $d = 467$.
Man finner $D(707) \equiv 707^{467} \equiv \cdots \equiv 718$ och $D(615) \equiv 615^{467} \equiv \cdots \equiv 719$

7. Vi gör fermattestet med bas 2: $2^{62} = (2^6)^{10} 2^2 = 64^{10} \cdot 4 \equiv 1^{10} \cdot 4 = 4 \neq 1 \pmod{63}$, så fermattestet ger att 63 inte är ett primtal.

8. Eftersom 101 är ett primtal och $101 \nmid 43$, gäller (Fermats lilla sats) att $43^{100} \equiv 1 \pmod{101}$ och $43^{139\,802} = (43^{100})^{1398} \cdot 43^2 \equiv 1^{1398} \cdot 1849 \equiv 31 \pmod{101}$.

9. Eftersom $341 = 11 \cdot 31$, där 11 och 31 är primtal, är (som i RSA, $k \in \mathbb{N}$) $43^{k(11-1)(31-1)+1} \equiv_{341} 43$ och $43^{139\,802} = (43^{466 \cdot 300 + 1}) \cdot 43 \equiv_{341} 43^2 = 1849 \equiv_{341} 144$.