1. Vi ska lösa den Diofantiska ekvationen $52x + 45y = 620$. Vi tar först fram en lösning till ekvationen $52x_0 + 45y_0 = 1$ genom att gå fram och baklänges i Euklides algoritm.

$$\begin{aligned} 52 &= 45 + 7 \\ 45 &= 6 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1, \end{aligned}$$

vilket ger

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ 1 &= 7 - 2(45 - 6 \cdot 7) = 13 \cdot 7 - 2 \cdot 45 \\ 1 &= 13(52 - 45) - 2 \cdot 45 = 13 \cdot 52 - 15 \cdot 45. \end{aligned}$$

Så $(13, -15)$ är en lösning till ekvationen $52x_0 + 45y_0 = 1$. För att få en lösning till den ursprungliga ekvationen multiplicerar vi med 620. Det ger en lösning $(13 \cdot 620, -15 \cdot 620) = (8060, -9300)$. Eftersom $SGD(52, 45) = 1$ blir den allmänna lösningen

$$\begin{cases} x = 8060 - 45k \\ y = -9300 + 52k, \end{cases}$$

där k är ett godtyckligt heltal. Då man inte kan handla ett negativt antal portioner måste $x \geq 0$ och $y \geq 0$. Det betyder att $8060 \geq 45k$ och $52k \geq 9300$, vilket ger

$$\frac{8060}{45} \geq k \geq \frac{9300}{52}.$$

Vi får därmed att $k = 179$. Insättning ger $(x, y) = (5, 8)$.
SVAR: Fem personer hade valt kött och åtta fisk.

2. Först väljer vi platser åt bokstöden. Eftersom det finns 10 böcker så finns det 9 platser att välja på. Det ger $\binom{9}{2}$. Sedan kan vi flytta om böckerna vilket ger 10!.
Svar: $10!\binom{9}{2}$.

3. Vi har att $n = 65 = 5 \cdot 13$, så $m = 4 \cdot 12 = 48$. För att dekryptera meddelandet behöver vi inversen till $e = 11$ modulo 48. Euklides algoritm ger

$$\begin{aligned} 48 &= 4 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 3 + 1 \end{aligned}$$

och går vi sedan baklänges får vi

$$\begin{aligned} 1 &= 4 - 3 \\ 1 &= 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 \\ 1 &= 3(48 - 4 \cdot 11) - 11 = 3 \cdot 48 - 13 \cdot 11. \end{aligned}$$

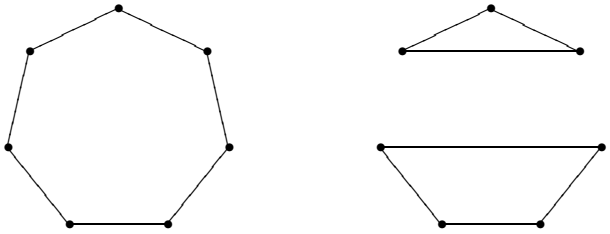
Vi får alltså att inversen blir $d = -13 \cong 35$. Det dekrypterade meddelandet ges nu av 2^{35} (mod 65). Vi har att

$$2^{35} \cong (2^6)^5 \cdot 2^5 \cong 64^5 \cdot 32 \cong (-1)^5 \cdot 32 \cong -32 \cong 33.$$

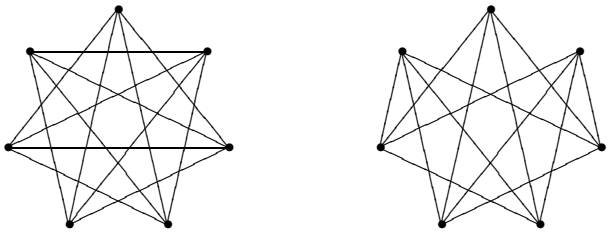
SVAR: Det dekrypterade meddelandet är “33”.

4. Talen 2, 3 och 5 är parvis koprima så en generator fås genom att ta elementet (x, y, z) där x är generator för C_2, y är generator för C_3 och z är generator för C_5. Om vi låter u vara generator för C_{30} så kan vi definiera vår isomorfi, ϕ, genom att sätta $\phi((x, y, z)) = u$. Det ger $\phi((x, y, z)^2 = (1, y^2, z^2)) = u^2$, $\phi((x, y, z)^3 = (x, 1, z^3)) = u^3$ o s v.

5. En reguljär graf är en där alla hörnen har samma valens. Eftersom antalet hörn med udda valens i en graf alltid är jämnt så är de enda möjliga fallen att grafen har valens 0, 2, 4 eller 6. Det första fallet är uteslutet då grafen förutsattes vara sammanhängande. Den enda sammanhängande reguljära grafen med valens 2 är den cykliska, så valens 2 ger C_7. Fallet med valens 6 är också lätt att behandla eftersom det betyder att varje hörn måste vara förbundet med varje annat hörn. Det återstår att behandla fallet då valensen är 4. För att göra det kan vi gå över till komplementet, som blir en reguljär graf med sju hörn och valens $7 - 4 - 1 = 2$. Skillnaden mot när vi tidigare tittade på valens två är att vi nu inte längre kan kräva att grafen är sammanhängande. Förutom det tidigare fallet har vi nu också möjligheten att grafen består av två cykler.



För att gå tillbaka ska vi dra kanter mellan de hörn som inte är förbundna i ovanstående grafer



Vi ser att bägge är sammanhängande och de kan inte vara isomorfa då komplementen ej var isomorfa så de ger de enda två 4-reguljära graferna med 7 hörn.

6. Två permutationer är konjugerade precis då de har samma typ. Frågan kan alltså omformuleras som: Hur många permutationer finns det i S_7 med typ [34]? Siffrorna 1 till 7 kan ordnas på 7! sätt. Om vi sedan grupperar de tre första och de fyra sista får vi permutationer av önskad typ. Två sådana permutationer är lika om någon av grupperingarna bara skiljer sig åt med en cyklisk permutering. Antalet sätt att cykliskt permutera inom parenteserna är 3 resp 4 så vi får totalt $\frac{7!}{3 \cdot 4}$ permutationer av typ [34].
SVAR: Det finns $\frac{7!}{3 \cdot 4}$ permutationer i S_7 som är konjugerade med $(123)(4567)$.

7. Eftersom gruppen har ordning 6 har elementen i gruppen ordning 1, 2, 3 eller 6. Om något element har ordning 6 så är gruppen isomorf med C_6. Om det skulle finnas två element i gruppen med ordning 2, säg a och b, så skulle $\{e, a, b, ab\}$ utgöra en delgrupp men den gruppen skulle få ordning 4 vilket är omöjligt då alla delgruppers ordningar måste dela gruppens ordning, se sats 13.8.2. Det ger att det högst finns ett element med ordning 2. Om gruppen inte är

den cykliska gruppen måste övriga element, utom enhetselementet, ha ordning 3. Men om det finns ett element av ordning 2 och ett av ordning 3 så är det lätt att se att deras produkt får ordning 6. Om vi inte vill få den cykliska gruppen måste vi därmed utesluta att något element har ordning 2. Anta så att alla element utom enhetselementet har ordning 3. Om vi betecknar elementen $\{e, a, b, c, d, f\}$ kan vi anta att $a^2 = b$ och $ac = d$. Då $bc = ad$ måste $ad = f$. Vi har så långt grupptabellen

e	a	b	c	d	f
a	b	e	d	f	c
b	e	a	f	c	d
c	d	f			
d	f	c			
f	c	d			

där vi har använt att gruppen är abelsk så grupptabellen är symmetrisk. Eftersom grupptabellen ska vara en latinskkvadrat ser vi att c^2 måste bli e, a eller b. Det första alternativet är uteslutet då vi antagit att c har ordning 3 men det utesluter även de andra alternativen för om $c^2 = a$ måste vi ha $ac = e$ om c ska ha ordning 3 men vi har $ac = e$. Motsvarande skulle $c^2 = b$ ge $bc = e$ men $bc = f$. Vi drar således slutsatsen att det inte kan finnas en abelsk grupp med ordning 6 som inte är isomorf med C_6.

8. Antalet avbildningar från en n-mängd till en k-mängd är som antalet ordnade val med repetition av k element ur en mängd med n element, dvs k^n stycken. Antalet sätt att träffa högst $k-1$ av elementen fås av $\binom{k}{1}(k-1)^n$. Vi har $\binom{k}{1}$ sätt att välja vilket element som inte träffas och sedan $(k-1)^n$ sätt att definiera avbildningar. Om vi drar bort det från det ursprungliga antalet får vi för lite för om en avbildning missar två element så räknas den dubbelt. Vi måste därmed lägga till $\binom{k}{2}(k-2)^n$. Men nu måste vi dra bort de som missar tre element, vilket är $\binom{k}{3}(k-3)^n$ stycken o s v.

9. För en kod som rättar 3 fel är minsta avståndet mellan två kodord $2 \cdot 3 + 1 = 7$ och för en linjär kod betyder det att vikten hos alla nollskilda kodord är 7, dvs de innehåller 7 ettor. Men om orden har längd 10 kommer två ord med sju ettor bara kunna skilja sig på 6 platser, vilket motsäger att minsta avståndet mellan två ord är 7. Däremot bildar ett godtyckligt ord med 7 ettor och nollordet en kod som rättar 3 fel, vilket visar att den maximala dimensionen är 1. För att en kod med längd tio ska rätta 2 fel krävs att minimala avståndet mellan två kodord är $2 \cdot 2 + 1 = 5$. Exempelvis har vi $\{0000000000, 1111100000, 0000011111, 1111111111\}$.

10. Låt $\phi(x) = ux$. Då är ϕ injektiv för om $\phi(x) = \phi(y)$ så är $ux = uy$ men multiplikation med u^{-1} ger $x = y$. Eftersom mängden är ändlig blir avbildningen även surjektiv, och därmed bijektiv. Det är alltså klart att ϕ ger en permutation av elementen i $\mathbf{Z}_m$. Vi ska nu visa att $\mathrm{SGD}(ux, m) = \mathrm{SGD}(x, m)$. Eftersom u och m saknar gemensamma delare så måste ett tal som delar både ux och m också dela x. Samtidigt är det klart att ett tal som delar x också delar ux vilket visar påståendet. Slutligen ska vi genomföra detta i praktiken för $\mathbf{Z}_{12}$. De inverterbara elementen i $\mathbf{Z}_{12}$ är 1, 5, 7 och 11. Multiplikation med 1 ger förstås identiteten. Multiplikation med 5 svarar mot permutationen $(0)(1\,5)(2\,10)(3)(4\,8)(6)(7\,11)(9)$, multiplikation med 7 mot $(0)(1\,7)(2)(3\,9)(4)(5\,11)(6)(8)(10)$ och multiplikation med 11 mot $(0)(1\,11)(2\,10)(3\,9)(4\,8)(5\,7)(6)$.