1. $\gcd(567, 417)$:

$$567 = 1(417) + 150$$
$$417 = 2(150) + 117$$
$$150 = 1(117) + 33$$
$$117 = 3(33) + 18$$
$$33 = 1(18) + 15$$
$$18 = 1(15) + 3$$
$$15 = 5(3) + 0$$

$$\underline{\underline{\gcd(567, 417) = 3}}$$

$$567x + 417y = \gcd(567, 417) = 3$$

Euklid baklengs

$$3 = 18 - 1(15)$$
$$= 18 - 1(33 - 1(18))$$
$$= 2(18) - 1(33)$$
$$= 2(117 - 3(33)) - 1(33)$$
$$= 2(117) - 7(33)$$
$$= 2(117) - 7(150 - 1(117))$$
$$= 9(117) - 7(150)$$
$$= 9(417 - 2(150)) - 7(150)$$
$$= 9(417) - 25(150)$$
$$= 9(417) - 25(567 - 1(417))$$
$$= 34(417) - 25(567)$$

$$x_0 = -25$$
$$y_0 = 34$$

$$\underline{\underline{x = -25 + \frac{417}{3}t = -25 + 139t}}$$

$$\underline{\underline{y = 34 - \frac{567}{3}t = 34 - 189t}}$$

2(a) $p^{2020} \pmod{10}$

$\gcd(10,p)=1$ når $p \neq 5$

Når $p \neq 0$

$p^{2020} \pmod{10}$

$\phi(10)=4$

$2020=4(505) \Rightarrow$

$p^{2020} \equiv (p^4)^{505} \equiv (1)^{505} \equiv 1 \pmod{10}$

Når $p=5$

$5^{2020} \pmod{10}$

$2020=1024+512+256+128+64+32+2+2$

$5^2 \equiv 25 \equiv 5 \pmod{10}$

$5^{32} \equiv (5^2)^{16} \equiv 5^{16} \equiv (5^2)^8 \equiv 5^8 \equiv (5^2)^4 \equiv 5^4 \equiv (5^2)^2 \equiv 5^2 \equiv 5 \pmod{10}$

$5^{64} \equiv (5^2)^{32} \equiv 5^{32} \equiv 5 \pmod{10}$

$5^{128} \equiv (5^2)^{64} \equiv 5^{64} \equiv 5 \pmod{10}$

$5^{256} \equiv (5^2)^{128} \equiv 5^{128} \equiv 5 \pmod{10}$

$5^{512} \equiv (5^2)^{256} \equiv 5^{256} \equiv 5 \pmod{10}$

$5^{1024} \equiv (5^2)^{512} \equiv 5^{512} \equiv 5$ (mod 10

$5^{2020} \equiv 5^{1024} \cdot 5^{512} \cdot 5^{256} \cdot 5^{128} \cdot 5^{64} \cdot 5^{32} \cdot 5^2 \cdot 5^2 \equiv 5^8 \equiv 5 \pmod{10}$

Det siste sifferet til p^{2020} er 1 når $p \neq 5$ og 5 når $p=5$

(b) $5^{2020} \pmod{7^2 \cdot 13}$

$\gcd(5, 7^2) = 1 = \gcd(5, 13)$

$7^2 \cdot 13 = 637$

$\phi(637) = (7^2 - 7) \cdot 12 = 504$

$2020 = 4(504) + 4$

$5^{4(504)} \equiv (5^{504})^4 \equiv 1^4 \equiv 1 \pmod{7^2 \cdot 13}$

$5^4 \equiv 625 \equiv -12 \pmod{7^2 \cdot 13} \Rightarrow$

$5^{2020} \equiv 5^{4(504)+4} \equiv 1 \cdot 5^4 \equiv -12 \pmod{7^2 \cdot 13}$

Vi får rest -12 når vi deler 5^{2020} på $(7^2 \cdot 13)$

(c) $7 \cdot (76!) \pmod{79}$

Wilson gir:

$77! \equiv 1 \pmod{79} \Rightarrow$

$7 \cdot 77 \cdot (76!) \equiv 7 \pmod{79}$

$77 \equiv -2 \pmod{79} \Rightarrow$

$(7 \cdot (76!))(-2) \equiv 7 \equiv 86 \pmod{79} \Rightarrow$

$7 \cdot (76!) \equiv -43 \equiv 36 \pmod{79}$

3. $\{n, e\} = \{143, 11\}$

$n = 11 \cdot 13$

$\phi(n) = 10 \cdot 12 = 120$

$ed = 11d \equiv 1 \pmod{120}$

$\gcd(120, 11) = 1$ ✓

$11d + 120y = 1$

Euklid:

$120 = 10(11) + 10$

$11 = 1(10) + 1$

$10 = 10(1) + 0$

Euklid baklengs:

$1 = 11 - 1(10)$

$= 11 - 1(120 - 10(11))$

$= 11(11) - 1(120)$

$\underline{\underline{d = 11}}$

Dekrypterer 5:

$5^{11} \pmod{143}$

$5^{11} \equiv 48828125 \equiv (341455 \cdot 143 + 60) \equiv 60 \pmod{143}$

<u>Den dekrypterte meldingen er 60</u>

4(a) $\phi(67)=66$

67 er et primtall og har derfor en primitiv rot

$\psi(n)$ = antall tall $\le p$ med orden n der $n \mid (p-1)$

Har lært at

$$\psi(n)=\phi(n)$$

$n=22 \Rightarrow$

$\phi(22)=1\cdot 10=10$

Det finnes 10 tall med orden 22 modulo 67 mellom 1 og 66

(b) $2^{\phi(18)} \equiv 1 \pmod{19}$

$\phi(18)=3^2-3=6$

5. Beviser at det finnes to forskjellige primtall S.A. p^2+20 også er et primtall

p,q forskjellige primtall

$p^2+20=c$, c primtall

$p=3$

6. $x^2 \equiv p \pmod{q}$

$\Rightarrow \left(\frac{p}{q}\right)=1$

$x^2 \equiv q \pmod{p}$

$$\left(\frac{q}{p}\right)=\begin{cases} \left(\frac{p}{q}\right), & p\equiv 1 \pmod{4} \text{ eller } q\equiv 1 \pmod{4} \\ -\left(\frac{p}{q}\right), & p\equiv q\equiv 3 \pmod{4} \end{cases}$$

$x^2\equiv q \pmod{p}$ har løsning hvis $p\equiv 1 \pmod{4}$ eller $q\equiv 1 \pmod{4}$

7. $\tau(n)=2020$

$\tau(p_1^{b_1}\cdot \ldots \cdot p_m^{b_m})=(b_1+1)\cdot\ldots\cdot(b_m+1)$

$2020=2^2\cdot 3\cdot 101$

$\tau(n)=(1+1)(1+1)(2+1)(100+1)$

For å få det minste tallet n må vi ta $n=2^{100}\cdot 3^2\cdot 4\cdot 5$