Elementær Talteori - Første aflevering

{St} Opgave 1.3

Prove that there are infinitely many primes of the form $6x - 1$.

Vi ved der er uendelige mange primtal.
Vi ved at alle tal har en unik primtalsfaktorisering.
Desuden ved vi alle tal kan skrives på formen $6x - r, r \in \{0, 1, 2, 3, 4, 5\}$.

Vi ser hurtigt, at hvis $r = \{0, 2, 3, 4\}$ er $6x - r$ dividerbart med enten 2 eller 3, og kan derfor ikke være et primtal.
Dette udelader primtallene $2, 3$ eller primtal på formen $6x - 5$ og $6x - 1$.
For at bevise at der uendelige mange på formen $6x - 1$ benytter vi modstrid. Antag at der findes en endelige mængde primtal, $p_1, p_2, .., p_n$, på formen $6x - 1$. Vi konstruerer herefter et tal $k = 6(p_1 p_2 .. p_n) - 1$, som altså selv har formen $6x - 1$.
Vi observerer at enhvert $p_i \nmid k$ da $p_i \mid (p_1 p_2 .. p_n) \mid 6(p_1 p_2 .. p_n)$ som medfører $p_i \mid 6(p_1 p_2 .. p_n)$, hvorved $p_i \nmid 6(p_1 p_2 .. p_n) - 1$ da denne difference skal være mindst 2 (det mindste primtal).
Dette betyder at k kan primfaktoriseres som $q_1 q_2 .. q_m$, hvor alle led er på formen $6x - 5$. Dog ses, at hvis alle led er på formen $6x - 5$ så er produktet også på formen $6x - 5$. Altså må der eksistere et primtal $p \notin (p_1, p_2, .., p_n)$ som er en primfaktor i k hvilket er en modstrid og der må altså eksistere uendelige primtal på formen $6x - 1$.

{St} Opgave 2.3

Use Algorithm 2.3.7 to find $x, y \in \mathbb{Z}$ such that $2261x + 1275y = 17$.

Vi bruger fremgangsmåden som er beskrevet i algoritme 2.3.7 {**St**}

$$
\begin{aligned}
2261 &= 1 * 1275 + 986 & \qquad 986 &= (1, -1) \\
1275 &= 1 * 986 + 289 & 289 &= (0, 1) - (1, -1) = (-1, 2) \\
986 &= 3 * 289 + 119 & 119 &= (1, -1) - 3(-1, 2) = (4, -7) \\
289 &= 2 * 119 + 51 & 51 &= (-1, 2) - 2(4, -7) = (-9, 16) \\
119 &= 2 * 51 + 17 & 17 &= (4, -7) - 2(-9, 16) = (22, -39) \\
51 &= 3 * 17 + 0 & 0 &= (-9, 16) - 3(22, -39) = (-75, 133)
\end{aligned}
$$

Derved bliver resten 0 og algoritmen terminerer. Her er $gcd(a, b) = d = 17$, som findes ved at tage a når algoritmen er termineret. En løsning findes ved at tage Bézout koefficienterne fra næstsidste række, nemlig $(x, y) = (22, 39)$, eller den generelle løsning

$$x = x_0 + \frac{bn}{d} = 22 + \frac{1275n}{17}$$
$$y = y_0 - \frac{an}{d} = -39 - \frac{2261n}{17}$$

Som er alle løsninger $x, y \in \mathbb{Z}$ til ligningen $2261x + 1275y = 17$.

{St} Opgave 2.10

Find an integer x such that $37x \equiv 1 \pmod{101}$

Vi starter med at bruge Euklids algoritme til at finde $gcd(37, 101)$.

$$\begin{aligned}
101 &= 2 * 37 + 27 \\
37 &= 1 * 27 + 10 \\
27 &= 2 * 10 + 7 \\
10 &= 1 * 7 + 3 \\
7 &= 2 * 3 + 1 \\
3 &= 3 * 1 + 0
\end{aligned}$$

Vi ser, at $gcd(37, 101) = 1$ og vi kan derfor substituere tilbage, for at finde et x til ligningen $37x - 101y = 1$.

$$\begin{aligned}
1 &= 7 - 2 * 3 = 7 - 2 * (10 - 7) = 3 * 7 - 2 * 10 \\
&= 3 * (27 - 3 * 10) - 2 * 10 = 3 * 27 - 8 * 10 \\
&= 3 * 27 - 8 * (37 - 27) = 11 * 27 - 8 * 37 \\
&= 11 * (101 - 2 * 37) - 8 * 37 = 11 * 101 - 30 * 37 \\
&= -30 * 37 + 11 * 101
\end{aligned}$$

Vi ser, at $x = -30$ er en løsning, da $-30 * 37 \equiv 1 \pmod{101}$, hvilket betyder -30 er en invers til 37 mod 101.

{St} Opgave 2.13

Find an $x \in \mathbb{Z}$ such that $x \equiv -4 \pmod{17}$ and $x \equiv 3 \pmod{23}$.

Vi vil bruge chinese remainder theorem til dette da ligningerne opfylder vi løser ligningssystemet

$$x \equiv a\,(mod\,m)$$
$$x \equiv b\,(mod\,n)$$

Hvor $a = 3, m = 23, b = -4, n = 17$.
Vi bruger algoritme 2.2.3 {**St**} til at finde et x. Et krav for at kunne bruge denne er at m og n er relativt primiske. Da både 17 og 23 er primtal, betyder det at dette er opfyldt. Vi kan så finde integers c, d så $cm + dn = 1$.

$$\begin{aligned} 23 &= 1 * 17 + 6 & 6 &= (1, -1) \\ 17 &= 2 * 6 + 5 & 5 &= (0, 1) - 2(1, -1) = (-2, 3) \\ 6 &= 1 * 5 + 1 & 1 &= (1, -1) - (-2, 3) = (3, -4) \\ 5 &= 5 * 1 + 0 & 0 &= (-2, 3) - 5(3, -4) = (-17, 23) \end{aligned}$$

Her finder vi c til 3 og d til -4. Anden del af algoritmen giver derved at

$$x = a + (b - a)cm = 3 + (-4 - 3) * 3 * 23 = -480$$

Som er det x der løser ligningsystemet.

Note: Ved dette x returnerer modolu operation altså -4 istedet for 13.

{JJ} Opgave 2.6

Prove that every prime $p \neq 3$ has the form $3q + 1$ or $3q + 2$ for some integer q; prove that there are infinitely many primes of the form $3q + 2$

Vi ved at alle tal kan skrives som $3q + r, r \in \{0, 1, 2\}$.
Vi ved der kun findes primtal p, hvor $p > 1$ hvilket betyder $q > 0$.

Derved har vi at alle tal med $r = 0$ er på formen $3q$ og altså må

- 3 gå op i tallet, og de kan derfor ikke være primtal.

- Tallet være 3.
- Tallet være 0.

Da 0 ikke er et primtal og 3 ikke er inkluderet i beviset, betyder det at alle primtal må være på formen $3q + 1$ eller $3q + 2$.

Vi vil vise, at der uendelige mange primtal på formen $3q + 2$ som er ækvivalent med $3q - 1$ da de rammer de samme tal. Dette gøres ved modstrid. Vi antager at der findes en endelig mængde primtal på formen $3q - 1$ noteret som $p_1, p_2, .., p_n$. Vi konstruerer nu et tal $k = 3(p_1p_2..p_n) - 1$ som også har formen $3q - 1$.
Af samme argumentation som i {**St, Opgave 1.3**} ser vi igen at enhvert $p_i \nmid k$ da $p_i \mid (p_1p_2..p_n) \mid 3(p_1p_2..p_n)$. Det medfører $p_i \mid 3(p_1p_2..p_n)$ og derved $p_i \nmid 3(p_1p_2..p_n) - 1$ da forskellen skal være mindst 2 da det er det mindste primtal.
Det betyder k kan primfaktoriseres som $q_1q_2..q_m$, hvor alle led er på formen $3q + 1$. Igen ses at hvis alle led er på formen $3q + 1$ så er produktet også på formen $3q + 1$. Der må derfor eksistere et primtal $p \notin (p_1, p_2, .., p_n)$ som er en primfaktor i k hvilket er en modstrid og der må altså eksistere uendelige primtal på formen $3q - 1$ og derved også $3q + 2$.

Note: Ideen med at omskrive $3q + 2$ til $3q + 1$ er for at undgå at k er på formen $3q + 2$, da en primtalsfaktor kunne være 2 som også har formen $3q + 2$.