Mat-1.128 DMP, 2. vk. 7.5.2002

1. $\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 7 \pmod{12} \\ x \equiv 13 \pmod{15} \\ x \equiv 11 \pmod{16} \end{cases} \Rightarrow$

$x = 3 + n\cdot 10 = 7 + m\cdot 12 \Rightarrow n\cdot 10 - m\cdot 12 = 4 \Rightarrow 5n - 6m = 2$

$n_0 = m_0 = -2 \Rightarrow n = -2 + 6k \Rightarrow x = 3 + 10(-2+6k) = -17 + 60k$

$x = -17 + 60k = 13 + 15h \Rightarrow 60k - 15h = 30 \Rightarrow 4k - h = 2$

$k_0 = 1,\ h_0 = 2 \Rightarrow k = 1 + r \Rightarrow x = -17 + 60(1+r) = 43 + 60r$

$x = 43 + 60r = 11 + 16s \Rightarrow 16s - 60r = 32 \Rightarrow 4s - 15r = 8$

$s_0 = 2,\ r_0 = 0 \Rightarrow r = 4t \Rightarrow x = 43 + 60\cdot 4t = 43 + 240\cdot t$

$\Leftarrow$ $x \equiv 43 \pmod{240}$

2. a) $9999 = 3^2 \cdot 11 \cdot 101 \Rightarrow \varphi(9999) = 9999\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{11}\right)\cdot\left(1-\frac{1}{101}\right) = 6000$

$9999 = 8\cdot 1201 + 391$, $1201 = 3\cdot 391 + 28$, $391 = 13\cdot 28 + 27$, $28 = 1\cdot 27 + 1 \Rightarrow$ s.y.t. $(1201, 9999) = 1$

Eulerin lause $\Rightarrow$ $1201^{6000} \equiv 1 \pmod{9999} \Rightarrow 1201^{12000002} \equiv \left(1201^{6000}\right)^{2000} \cdot 1201^2 \equiv 1201^2 \equiv \underline{\underline{2545}} \pmod{9999}$

b) $n = pq = 106481$, $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = 105792 \Rightarrow$

$p+q = 106481 - 105792 + 1 = 690$, $p-q = \sqrt{(p+q)^2 - 4pq} = \sqrt{690^2 - 4\cdot 106481} = 224 \Rightarrow$

$p = \frac{1}{2}(690 + 224) = \underline{\underline{457}}$, $q = \frac{1}{2}(690 - 224) = \underline{\underline{233}}$

3. a) $GF(25) = GF(5^2) \Rightarrow$ Tarvitaan astetta 2 oleva redusoitumaton $\mathbb{Z}_5$-polynomi.

Esim. $s(u) = u^2 - 2$: $s(0) = -2 \neq 0$, $s(\pm 1) = (\pm 1)^2 - 2 = 1 - 2 = -1 \neq 0$, $s(\pm 2) = (\pm 2)^2 - 2 = 4 - 2 = 2 \neq 0$

(Huom. Muitakin vaihtoehtoja on, esim. $u^2 + 2$ kelpaa, mutta $u^2 + 1 = u^2 - 4 = (u-2)(u+2)$ tai $u^2 - 1 = (u-1)(u+1)$ ei sovellu, jne. On olemassa 10 kpl, redusoitumattomia 2. asteen polynomeja. Jos valitaan jokin muu kuin $s(u) = u^2 - 2$, muuttuu a)- ja b)-kohtien vastausten muoto.) $\Rightarrow$

$GF(25) = \{a + bu \mid a, b \in \mathbb{Z}_5,\ u^2 = 2\}$

b) $f(x) = x^4 + 1 \in GF(25)$: $x^4 + 1 = x^4 - 4 = (x^2 - 2)(x^2 + 2) = g(x)\cdot h(x)$

Edelleen: $g(\pm u) = (\pm u)^2 - 2 = u^2 - 2 = 0$, $h(\pm 2u) = (\pm 2u)^2 + 2 = 4\cdot 2 + 2 = 10 = 0 \Rightarrow$

$f(x) = x^4 + 1 = (x-u)(x+u)(x-2u)(x+2u)\ (= (x-u)(x-2u)(x-3u)(x-4u) = \cdots)$

4. $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \Rightarrow G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \Rightarrow$

a) $(1001)G = \underline{1001001}$, $(0111)G = \underline{0111000}$

b) $H\cdot(1010010)^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow$ ei havaittu virhettä $\Rightarrow c_1 = 1010010 \Rightarrow \underline{w_1 = 1010}$

$H\cdot(1010100)^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \Rightarrow$ havaittu virhe $= \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ on H:n 4. pystyrivi $\Rightarrow$ korjataan 4. bitti $\Rightarrow c_2 = 1011100 \Rightarrow \underline{w_2 = 1011}$

c) $P = 1 - \left((p-1)^7 + \binom{7}{1}\cdot(p-1)^6\cdot p\right)^2 = 1 - \left(0.9925^7 + 7\cdot 0.9925^6\cdot 0.0075\right)^2 = 0.0023\ldots \approx \underline{0.23\ \%}$