T-79.5501 Cryptology
Exam
December 14, 2005

SOLUTIONS

1. By Corollary 2.9 we have $\mathrm{H}(\mathbf{K}|\mathbf{C}) \leq \mathrm{H}(\mathbf{K})$ with equality if and only if $\mathbf{K}$ and $\mathbf{C}$ are independent. On the other hand, by the result of Theorem 2.10, we have $\mathrm{H}(\mathbf{K}|\mathbf{C}) = \mathrm{H}(\mathbf{K})$ + $\mathrm{H}(\mathbf{P})$ - $\mathrm{H}(\mathbf{C})$. By combining these two results we get the what is claimed.

2. First we find integers s and t such that $14s + 2005t = 1$ using Euclid's algorithm. We get $s = -716$ and $t = 5$. Then $x_0 = 12s = -8592$ and $y_0 = 12t = 60$ satisfy the given equation. All solutions are pairs (x_n, y_n), $n \in \mathbb{Z}$, where $x_n = x_0 - 2005n$ and $y_n = y_0 + 14n$. For example, one such solution is $x_{-4} = -572$, $y_{-4} = 4$.

3. (a) Since $g(x)$ is irreducible and $f(x)$ is not a multiple of $g(x)$ we get $\mathrm{lcm}(f(x), g(x)) = f(x)g(x) = x^7 + 1$.

   (b) From (a) and Theorem 2 of Lecture 4 it follows that the sum sequence $S_1 + S_2$ can be generated using an LFSR with connection polynomial $\mathrm{lcm}(f(x), g(x)) = x^7 + 1$. Clearly the exponent of $x^7 + 1$ is equal to 7. By Theorem 3, Lecture 4, the period of $S_1 + S_2$ divides 7. Since $g(x)$ is primitive, the nonzero sequences S_2 it generates have period $2^3 - 1 = 7$. Hence 7 is the largest period the sum sequence $S_1 + S_2$ can have.

4. (a)
$$\left(\frac{1223}{2005}\right) = \left(\frac{782}{1223}\right) = \left(\frac{391}{1223}\right) = -\left(\frac{50}{391}\right) = -\left(\frac{25}{391}\right) = -\left(\frac{16}{25}\right) = -1.$$

   (b)
$$\begin{aligned} 1223^{\frac{2005-1}{2}} \bmod 2005 &= 1223^{1002} \bmod 2005 \\ &= \begin{cases} 3^2 \bmod 5 = -1 \bmod 5 \\ 20^{202} \bmod 401 = (-1)^{101} \bmod 401 = -1 \bmod 401 \end{cases} \end{aligned}$$

   By the Chinese Remainder Theorem we get $1223^{\frac{2005-1}{2}} \bmod 2005 = -1$. Then it follows from (a) that
$$\left(\frac{1223}{2005}\right) \equiv 1223^{\frac{2005-1}{2}} \pmod{2005}$$
   as desired.

5. (a) Bob decrypts by computing $a_1 = 38176^{\frac{131+1}{4}} \bmod 131 = 102$ and $a_2 = 38176^{\frac{311+1}{4}} \bmod 311 = 168$, and combines these using the Chinese Remainder Theorem to get four possible decryptions:
$$\begin{aligned} x &= \pm 102 \cdot 311 \cdot (311^{-1} \bmod 131) \pm 143 \cdot 131 \cdot (131^{-1} \bmod 311) \bmod 40741 \\ &= 1412,\ 20072,\ 20669,\ 39329, \end{aligned}$$
   where Bob computes $311^{-1} \bmod 131 = -8$ and $131^{-1} \bmod 311 = 19$ using Euclid's algorithm. From the four possible decryptions $x_1 = 1412$ is the date of this exam.

   (b) Alice gets to know that $1412^2 \equiv 20669^2 \bmod 4071$. She then computes $\gcd(20669 - 1412, 40741) = 131$, and gets $40741 = 131 \cdot 311$.