T-79.159 Cryptography and Data Security
2005 / Homework 5
Tue 19.4 and Fri 22.4

1. Use the Square-and-Multiply algorithm to compute 5^{11}
   (a) in modulo 2005 arithmetic; and
   (b) in polynomial arithmetic modulo $f(x) = x^4 + x + 1$
2. Why isn't $\mathbb{Z}_n$ a field when n isn't a prime. Which property fails?
3. Let us define an operation in the set of 16-bit integers as follows. Given two sixteen-bit integers compute first their product modulo $2^{16} + 1$. If the result is equal to 2^{16} it is encoded as zero. How many zeros are there in the resulting table for this operation? (Note that this is different from the IDEA operation that makes use of multiplication modulo $2^{16} + 1$. In IDEA, before multiplication is computed, an all-zero 16-bit string is replaced by the number 2^{16}.)
4. In the round key expansion procedure Rijndael makes use of constants C_i, $i = 1, 2, 3, ..., 30$ that can be computed as

   $$C_i = 2^{i-1}$$

   in polynomial arithmetic modulo $m(x) = x^8 + x^4 + x^3 + x + 1$. Compute C_{11}, C_{12} and C_{13}.
5. Show that the multiplicative order of $g = 8 = 2^3$, in modulo 19 arithmetic, is equal to 6.
6. Alice and Bob use Diffie-Hellman in the cyclic group of order 18 generated by $g = 2$ in modulo 19 arithmetic. Alices secret exponent $a = 7$ and Bob's secret exponent $b = 5$. Compute the Diffie-Hellman key K.