

Mathematics of Coding and Cryptography
Worksheet 11

1. Factor 171 and 297 using Fermat factorization.
2. Use Miller-Rabin with $a = 2$ to determine which of the following integers are composite:
 - (a) 3277
 - (b) 10002
 - (c) 5477
 - (d) 3491
3. Show that $n = 3277$ is a strong pseudoprime for the base 2 by showing that it factors using the $p - 1$ factorization algorithm for $B = 8$.
4. Suppose you know $n = 280801$ is the product of two primes. Use the $p - 1$ factoring algorithm to factor it.
5. Factor $n = 16843009$ using the quadratic sieve and the following congruences:

$$4122^2 \equiv 5^3 \cdot 7 \cdot 13^2 \pmod{n}$$

$$4159^2 \equiv 2^7 \cdot 3 \cdot 7 \cdot 13^2 \pmod{n}$$

$$4187^2 \equiv 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 13 \pmod{n}$$

$$4241^2 \equiv 2^5 \cdot 3^6 \cdot 7^2 \pmod{n}$$

$$4497^2 \equiv 2^5 \cdot 5^4 \cdot 13^2 \pmod{n}$$

$$4993^2 \equiv 2^9 \cdot 3^5 \cdot 5 \cdot 13 \pmod{n}.$$