University of Limerick
Department of Mathematics and Statistics
Dr. S. Franz

OLLSCOIL LUIMNIGH
UNIVERSITY OF LIMERICK

MA4016 - Engineering Mathematics 6

Problem Sheet 7: Number Theory (March 19, 2010)

The algorithm for fast modular exponentiation can also be done by hand.
Example: Find 3^{340} mod 341. Note that $340 = 256 + 64 + 16 + 4 (= 2^8 + 2^6 + 2^4 + 2^2)$.
We compute

$$\begin{aligned}
3^1 \bmod 341 &= 3\\
3^2 \bmod 341 &= 9\\
3^4 \bmod 341 &= 9^2 \bmod 341 = 81\\
3^8 \bmod 341 &= 81^2 \bmod 341 = 82\\
3^{16} \bmod 341 &= 82^2 \bmod 341 = 245\\
3^{32} \bmod 341 &= 245^2 \bmod 341 = 9\\
3^{64} \bmod 341 &= 81\\
3^{128} \bmod 341 &= 82\\
3^{256} \bmod 341 &= 245
\end{aligned}$$

and

$$3^{340} \bmod 341 = 81{\cdot}245{\cdot}81{\cdot}245 \bmod 341 = (81^2 \bmod 341)(245^2 \bmod 341) = 82{\cdot}9 \bmod 341 = 56$$

1. Find 11^{644} mod 645 and 123^{1001} mod 101 using fast modular exponentiation.

2. Solve the congruence $2x \equiv 7 \bmod 17$.

3. Find all solutions to the system of congruences.

$$x \equiv 2 \pmod 3, \quad x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 5.$$

4. Find all solutions, if any, to the system of congruences.

$$x \equiv 5 \pmod 6, \quad x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}.$$

5. **a)** Use Fermat's Little Theorem to compute 3^{302} mod 5, 3^{302} mod 7, and 3^{302} mod 11.

b) Use the results from part **a)** and the Chinese Remainder Theorem to find 3^{302} mod 385. Note that $305 = 5 \cdot 7 \cdot 11$.

6. Suppose that we choose for the RSA-cryptosystem the primes $p = 17$ and $q = 23$, and the encryption exponent $e = 31$. Compute n, $\varphi(n)$ and d. Encrypt 101 and decrypt 250 using above parameters.