

Worksheet on Modular Exponentiation

Dr. Holmes

April 23, 2010

Compute these powers in the indicated moduli by the method of repeated squaring (with adjustments for odd exponents) that I demonstrated in class.

1. Compute $8^{128} \bmod 100$. This is really easy (why?)
2. Compute $10^{111} \bmod 137$
3. Compute $3^{100} \bmod 17$ by the repeated squaring method, *before* looking at the simpler calculation in the next paragraphs.

By Fermat's little theorem, $3^{16} \bmod 17 = 1$

Notice that this means that $3^{16x} = (3^{16})^x = 1^x = 1$ in mod 17 arithmetic. This means that $3^{100} = 3^{96}3^4 = (3^{16})^63^4 = 1^63^4 = 3^4 = 81$ in mod 17 arithmetic, so $3^{100} = 3^4 = 81 - (4 * 17) = 13$ in mod 17 arithmetic. The point here is the we can reduce the exponent (100) to its remainder (4) on division by $16 = 17-1$, because the modulus we are working in (17) is prime.

Notice that this only works because 17 is prime. Compare this calculation with the repeated squaring calculation of the same value that you did above.

4. Compute $10^{221} \bmod 13$ by repeated squaring.

Then compute the same value using Fermat's little theorem as in the calculation I just gave in the previous part (you might do a little repeated squaring after the simplification). The fact you are going to use is that by Fermat's little theorem, $10^{12} = 1 \bmod 13$, so we can reduce exponents to their remainders mod 12 when computing exponentials in mod 13 arithmetic.

5. Give numbers x, y, z such that $y \bmod 5 = z \bmod 5$ but $x^y \bmod 5 \neq x^z \bmod 5$