MATH 104A NUMBER THEORY - FINAL WINTER 2000

Instructor: Wenzl

1. Compute the smallest residue of 47^{2521} mod 155.
4. Find a primitive root mod $343 = 7^3$. Justify your steps.
5. A message is encoded via the Pohlig-Hellman exponentiation code using the prime 2591 and exponent $e = 13$, i.e. a number $M < 2591$ is encoded to a number C via $C \equiv M^{13}$ mod 2591. Compute the exponent d for decoding it.
6. For the following Diophantine equation, either find all solutions or show that there exist no solutions: $60x + 18y = 97$.
7. (a) Prove that the equation $x^3 \equiv 1$ mod p only has one solution if p is a prime such that $p \equiv 2$ mod 3.
   (b) Prove that if a is a solution of $x^3 \equiv 1$ mod n, then so is a^2.
8. Compute all solutions of $x^3 - 1 \equiv 0$ mod 1313.(*Hint*: You can use the statements of Problem 7 regardless whether you could do it or not.)