MATH 195: CRYPTOGRAPHY
HOMEWORK #3

Problem 7.8. *Recall* $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$. *Give a concise reason why* $\phi(n)$ *is even for* $n > 2$.

Problem 7.9(a). *Determine* $\gcd(24140, 16762)$.

Problem 7.9(b). *Determine* $\gcd(4655, 12075)$.

Problem 7.9(c). *Compute* 367^{-1} *in* $(\mathbb{Z}/1001\mathbb{Z})^*$ *and* 1001^{-1} *in* $(\mathbb{Z}/367\mathbb{Z})^*$.

Problem 2.11. *For which* n *is the matrix*

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}$$

invertible over $\mathbb{Z}/n\mathbb{Z}$? *Find its inverse if* $n = 100$.

Problem 2.12. *Exhibit an algorithm that given a prime number* n *and a* $k \times k$ *matrix* M *over* $\mathbb{Z}/n\mathbb{Z}$, *computes* $\det M$ *using no more than* k^3 *arithmetic operations* $(+, -, \cdot, ^{-1})$ *in* $\mathbb{Z}/n\mathbb{Z}$, *of which no more than* k *are inversions* $(^{-1})$.

Date: February 12, 2002.

7.8, 7.9(a)(b)(c), 2.11, 2.12.