

Prof. Valentin Blomer

University of Toronto Mississauga
Department of Mathematical and Computational Sciences

Introduction to Number Theory

Problem Set 6 (due Feb 26, 2008)

6.1. Write down a multiplication table for $(\mathbb{Z}/9\mathbb{Z})^*$. What are the orders of the elements? Does there exist a primitive root?

6.2. Let $n \in \mathbb{N}$. Show that a linear map $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $[x] \mapsto [ax + b]$ is invertible if and only if $\gcd(a, n) = 1$.

Hints: For the “if”-part use that our assumption implies that $[a]$ is a unit, hence there is some $[r]$ with $[a][r] = [1]$. Now construct explicitly an inverse map. For the “only-if”-part look at a preimage of $[b + 1]$.

6.3. Suppose you want to use the two prime numbers $p_1 = 1637$ and $p_2 = 2203$ for the RSA public key cryptosystem. As your public key you use the pair $(n, e) = (3606311, 1440989)$, and keep as your private information that $n = p_1 p_2$. Now your friend sends you the following message:

1190411 2311965 3118717..

Calculate $\phi(n)$ and d and decode the three numbers. Decipher the text as follows: Each number corresponds to a word. Write each decoded number as $\sum_{j \geq 0} a_j 26^j$ with $a_j \in \{0, 1, \dots, 25\}$ with the interpretation

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

For example, $16346 = 18 + 26 \cdot 4 + 676 \cdot 24$ means YES. Feel free to use a pocket calculator or a computer or an online calculator, e.g. www.math.com/students/calculators/source/basic.htm.

6.4. Characterize all integers $n \in \mathbb{N}$ with the property $4 \nmid \phi(n)$ in terms of their prime power factorization. *Hint:* Use the explicit formula for $\phi(n)$.