

# Lectures on Challenging Mathematics

## Math Olympiads

## Number Theory

Summer 2018

Zuming Feng

Phillips Exeter Academy and IDEA Math

zfeng@exeter.edu

©Copyright 2008 – 2018 Idea Math

# Contents

©Copyright 2008 – 2018 Idea Math

<b>1</b>	<b>Number Theory</b>	<b>3</b>
1.1	Warm-up . . . . .	3
1.2	Complete set of residue classes . . . . .	4
1.3	Modular inverse . . . . .	6
1.4	Wilson’s theorem . . . . .	7
1.5	Modular arithmetic (part 1) . . . . .	8
1.6	Complications in solving linear congruence . . . . .	9
1.7	Modular arithmetic (part 2) . . . . .	10
1.8	Modular arithmetic (part 3) . . . . .	11
1.9	Modular arithmetic (part 4) . . . . .	12
1.10	Lagrange’s Interpolation Formula and Chinese Remainder Theorem . . . . .	13
1.11	Modular arithmetic (part 5) . . . . .	14
1.12	Fermat’s Little Theorem . . . . .	15
1.13	Proofs in modular arithmetic (part 1) . . . . .	16
1.14	Euler’s theorem . . . . .	17
1.15	Proofs in modular arithmetic (part 2) . . . . .	18
1.16	Modular arithmetic (part 6) . . . . .	19
1.17	Proofs in modular arithmetic (part 3) . . . . .	20
1.18	Quadratic residues . . . . .	21
1.19	Proofs in modular arithmetic (part 4) . . . . .	22
1.20	Diophantine equations . . . . .	23
<b>2</b>	<b>Practice Tests</b>	<b>25</b>
2.1	MO2M2 practice test 1 . . . . .	25
2.2	MO2M2 practice test 2 . . . . .	26
2.3	MO2M2 practice test 3 . . . . .	27
2.4	MO2M2 practice test 4 . . . . .	28
2.5	MO2M2 practice test 5 . . . . .	29

## 1.15 Proofs in modular arithmetic (part 2)

1. Let  $p$  be an odd prime, and let  $a$  and  $b$  be two relatively prime positive integers. Find the set of all possible values of

$$\gcd\left(a + b, \frac{a^p + b^p}{a + b}\right).$$

2. Let  $S(x)$  be the sum of the digits of the its decimal representation.

(a) Prove that for every positive integer  $x$ ,  $\frac{S(x)}{S(2x)} \leq 5$ . Can this bound be improved?

(b) Prove that  $\frac{S(x)}{S(3x)}$  is not bounded.

3. Call a number *very composite* if it has at least 2008 distinct prime factors. Do there exist 2008 consecutive very composite numbers?

4. Tanya chooses a positive integer  $x \leq 100$ , and Sasha is trying to guess this number. She can select two positive integers  $m$  and  $n$  less than 100 and ask for the value of  $\gcd(x + m, n)$ . Show that Sasha can determine Tanya's number with at most seven questions (the numbers  $m$  and  $n$  can change each question).

5. Find all primes  $p$  such that  $(p - 1)! + 1$  is a perfect power of  $p$ .