**Homework 3** Due 18:00, October 27, 2021

Cristian Brinza FAF 212

# Problem 4.1

Read the amazing story on the proof of Fermat Theorem from Simon Singh blog post “The whole Story”. The link is provided on the course web page on ELSE platform.

# Problem 4.2

Prove the following properties for any integers *a, b*:

1. gcd(*ka, kb*) = *k ·* gcd(*a, b*) for all *k >* 0.
2. If gcd(*a, b*) = 1 and gcd(*a, c*) = 1, then gcd(*a, bc*) = 1.
3. If *a | bc* and gcd(*a, b*) = 1, then *a | c*.

# Problem 4.3

A number is called **perfect** if it is equal to the sum of its positive divisors, other than itself. For example, 6 = 1 + 2 + 3 or 28 = 1 + 2 + 4 + 7 + 14 are perfect numbers.

Explain why 2*k−*1(2*k −* 1) is perfect, when 2*k −* 1 is a prime number.

# Problem 4.4

Use the Extended Euclid Algorithm (Pulverizer) to find the greatest common divisors and integers *st* and *t*

such that

1. gcd(60*,* 21) = *s ·* 60 + *t ·* 21;
2. gcd(42*,* 360) = *s ·* 42 + *t ·* 360.

# Problem 4.5

Let *m* = 295241171712 and *n* = 2372211211131179192.

What is the gcd(*m, n*)?

# Problem 4.6

Let *n* = 11 and consider modular classes modulo 11 (denoted by [*x*]). Compute:

1. [4] + [8] ;

**b)** [3] *−* [9];

**c)** [6] *·* [5] ;

**d)** [8]*−*1;

**e)** [7] *·* [6]*−*1 .

**f)** [5] *−* [10]*−*1.

# Problem 4.7

Repeat previous problem with *n* = 12. Compute:

1. [4] + [8] ;

**b)** [3] *−* [9];

**c)** [6] *·* [5] ;

**d)** [8]*−*1;

**e)** [7] *·* [6]*−*1 ;.

**f)** [5] *−* [10]*−*1.

# Problem 4.8

1. Use the Extended Euclid Algorithm (Pulverizer) to find the multiplicative inverse of 19 modulo 31 in the range *{*0,. . . ,30*}*.
2. Use Little Fermat Theorem to find the multiplicative inverse of 19 modulo 31 in the range *{*0,. . . ,30*}*.

c) Compute 19147 modulo 17.

# Problem 4.9

Let *ϕ*(*n*) be the totient function (Euler function). Find

a) *ϕ*(18);

b) *ϕ*(170;

c) *ϕ*(400) .