Homework $15^{-1} \pmod{59}$

Due X^*/Y^*, at Z^*:00 2023

Problem 4.1

First of all, you need to find out when this homework is due! It might be due tomorrow. To find it out decrypt message $X^*/\ Y^*$ and Z^* with

$$\begin{aligned} X^* &= 72747 \\ Y^* &= 23069 \\ Z^* &= 38826 \end{aligned}$$

given that it was encrypted with RSA algorithm with public key $(e, n) = (1741, 89951)$. Show your work! (in other words, show how you will compute the decryption key, etc). Notice, that if you wouldn't know the factorization of $n = 89951$, then it is extremely hard to compute the decryption key.

REMARK. In this homework you might need calculators for arithmetic operations on large numbers as well as tools for primality checking, since standard scientific calculators will be of no help in most of these cases. There are several such large number calculators and applets available online. Let Google be with you!

Problem 4.2

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 4.3

Prove the following properties for any integers a, b:

a) $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.

b) If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

c) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Problem 4.4

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 4.5

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

a) $\gcd(60, 21) = s \cdot 60 + t \cdot 21$;

b) $\gcd(42, 360) = s \cdot 42 + t \cdot 360$.

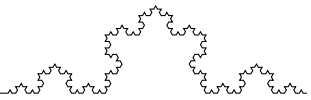
Problem 4.6

Let $m = 2^9 5^{24} 11^7 17^{12}$ and $n = 2^3 7^{22} 11^{211} 13^1 17^9 19^2$.

What is the $\gcd(m, n)$?

Problem 4.7

Let $n = 13$ and consider modular classes modulo 13 (denoted by $[x]$). Compute:



a) $[4] + [9]$;
b) $[3] - [8]$;
c) $[6] \cdot [7]$;
d) $[8]^{-1}$;
e) $[7] \cdot [6]^{-1}$.
f) $[5] - [10]^{-1}$.

Problem 4.8
Repeat previous problem with $n = 12$.

Problem 4.9
a) Use the Extended Euclid Algorithm (Pulverizer) to find the multiplicative inverse of 19 modulo 47 in the range $\{0,\ldots,46\}$.

b) Use Little Fermat Theorem to find the multiplicative inverse of 19 modulo 47 in the range $\{0,\ldots,46\}$.

c) Compute 19^{147} modulo 13.

Problem 4.10
Let $\varphi(n)$ be the totient function (Euler function). Find

a) $\varphi(28)$;

b) $\varphi(175)$;

c) $\varphi(420)$.

Problem 4.11
Security and Information Agency from Republic of Moldova (SIS) have intercepted a codified message from a very dangerous group of hackers. First message probably was codified using a permutation or substitution cipher. Decipher it:

FG LTEKTZL STYZ YGK TBETHZOGFQS LZXRTFZL YKGD
LGYZVQKT TFUOFTTKOFU AFGVF QL YQY YKGD XZD

Problem 4.12
On another occasion, SIS intercepted from the same group of criminals the following 58−digit long message:

60140590722316491443846160417575135526622059243409026478 19

It is known that this evil group uses the following encryption table (the simpler the better)

$A = 01$	$J = 10$	$S = 19$	$* = 28$	$2 = 37$
$B = 02$	$K = 11$	$T = 20$	$) = 29$	$3 = 38$
$C = 03$	$L = 12$	$U = 21$	$! = 30$	$4 = 39$
$D = 04$	$M = 13$	$V = 22$	$:= 31$	$5 = 40$
$E = 05$	$N = 14$	$W = 23$	$(= 32$	$6 = 41$
$F = 06$	$O = 15$	$X = 24$	$- = 33$	$7 = 42$
$G = 07$	$P = 16$	$Y = 25$	$+ = 34$	$8 = 43$
$H = 08$	$Q = 17$	$Z = 26$	$! = 35$	$9 = 44$
$I = 09$	$R = 18$	$space = 27$	$1 = 36$	$0 = 45$

Confidential sources told SIS that a Turing 1.0 algorithm have been used with encryption key being the smallest 6−digit prime number with the sum of its digits = 13. Decrypt the message and help your country!

Problem 4.13

Later, SIS intercepted (lucky them!) other two messages
(encrypted with a key different from the one previously used):

$$182849743138009657693006 9$$

$$214769443120931514639320840852363$$

Decrypt both messages, since they might give hints about the possible identity and location of their leader!

Problem 4.14

Consider Turing 2.0 algorithm with $p = 503$.

a) Encrypt message $m = 475$ with secret key $k = 127$.

b) Recover the original message m sent with secret key $k = 6$ if the received message $m^* = 443$.

Problem 4.15

Consider Turing 2.0 algorithm with $p = 13$. The secret key is not known, but you have intercepted both messages $m = 8$ and $m^* = 4$. Find the secret key k.