1. (5 points) What is the value of the sum

$$\sum_{j=0}^{8} 3 \cdot 2^j?$$

We have that for any geometric series $\sum_{j=0}^{n} a r^j = \frac{a r^{n+1} - a}{r-1}$ if $r \neq 1$

Let $a = 3$ and $r = 2$ we get

$$\sum_{j=0}^{8} 3 \cdot 2^j = \frac{3 \cdot 2^9 - 3}{2-1} = 3(2^9 - 1) = 3(512-1) = 3 \times 511 = 1533$$

2. (10 points) Find the prime factorization of 12!. *(Note that ! stands for factorial.)*

$$13! = 13 \times 12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2$$

$$= 13 \times \cancel{2}^2 \times \cancel{3} \times \cancel{11} \times \cancel{5} \times \cancel{2} \times \cancel{3}^2 \times \cancel{2}^3 \times \cancel{7} \times \cancel{2} \times \cancel{3} \times \cancel{5} \times \cancel{2}^2 \times \cancel{3} \times 2$$

$$= 13 \times 11 \times 7 \times 5^2 \times 3^5 \times 2^{10}$$

3. What is the cardinality of the following sets? (Is it finite? Is it countable? Is it uncountable?)

   (a) (5 points) $\{x \mid x/2 \text{ is an integer}\}$

   (b) (5 points) $\{x \mid x/2 \text{ is a positive integer less than } 10\}$

   (c) (5 points) $\{x \mid \lfloor x \rfloor = 0\}$
   (Note that $\lfloor x \rfloor$ denotes the floor function.)

a) $\{x \in \mathbb{Z} \mid x/2 \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x = 2k,\ k \in \mathbb{Z}\}$

$=$ set of even integers

this is an infinite countable set

b) $\{x \in \mathbb{Z} \mid x/2 \in \mathbb{Z}^+ \text{ and } x/2 < 10\} = \{2, 4, 6, 8, 10, 12, 14, 16, 18\}$

Cardinality is equal to $\underline{9}$.

c) $\{x \in \mathbb{R} \mid \lfloor x \rfloor = 0\} = [0, 1) = [0, 1] - \{1\}$

We have shown $[0, 1]$ is uncountable, therefore $[0, 1] - \{1\}$ is uncountable.

4. Show that

(a) (4 points) $\frac{x^6+2x^3+x^2+1}{x^3+1}$ is $O(x^3)$.

(b) (6 points) $\frac{x^6+2x^3+x^2+1}{x^3+1}$ is not $O(x^2)$.

(a) Show $\exists C, k$ s.t. $\left|\frac{x^6+2x^3+x^2+1}{x^3+1}\right| \leq C|x^3|$ when $|x|>k$

(let $k>0$, so that we can remove the abs. value signs)

$x^3+1 > x^3 \Rightarrow \frac{1}{x^3+1} < \frac{1}{x^3}$

$x^6+2x^3+x^2+1 \leq x^6+2\cdot x^6+x^6+x^6 = 5x^6$ when $x \geq 1$

(so now let $k \geq 1$)

$\frac{x^6+2x^3+x^2+1}{x^3+1} < \frac{5x^6}{x^3} = 5x^3$. Done — let $k=1$ $C=5$

(b) Proof by contradiction.

Assume there are C & k s.t.

$\frac{x^6+2x^3+x^2+1}{x^3+1} < Cx^2$. We must find an x

$x^3+1 \leq x^3+x^3=2x^3 \Rightarrow \frac{1}{x^3+1} \geq \frac{1}{2x^3}$

$x^6+2x^3+x^2+1 > x^6$ when $x \geq 0$

$\Rightarrow \frac{x^6+2x^3+x^2+1}{x^3+1} > \frac{x^{\cancel{6}3}}{2x^3} = \frac{1}{2}x^3$ when $x \geq 0$

Pick $x > \max(2C, k)$. $\frac{x^2+2x^3+x^2+1}{x^3+1} > \frac{1}{2}x\cdot x^2 > \frac{2C}{2}\cdot x^2 = Cx^2$

contradition!

So no such C, k can exist.

5. (10 points)

Show that if a, b, c, and d are integers such that $a|c$ and $b|d$, then $ab|cd$.

$a|c$ means $c = am$ for $m \in \mathbb{Z}$

$b|d$ means $d = bp$ for $p \in \mathbb{Z}$

want to show that $ab|cd$ i.e: $cd = ab \times q$ for some $q \in \mathbb{Z}$

by assumption $c.d = a.m \times b.p = ab(mp)$ and $mp \in \mathbb{Z}$.

6. (15 points)

Input: b: positive integer, $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$: positive integer,
m: positive integer

Output: x: positive integer. x equals b^n **mod** m

x:=1;
power:=b **mod** m;
foreach $i := 0$ *to* $k-1$ **do**
  if a_i=1 **then**
    $x := (x \cdot power)$ **mod** m;
  end
  $power := (power \cdot power)$ **mod** m;
end

Algorithm 1: Modular exponentiation

How many multiplications are used by Algorithm 1 to calculate 5^{33} **mod** 7?

$b=5$, $n = 33 = (1\,0\,0\,0\,0\,1)$ $k-1=5$ $m=7$

a_5 $a_1\, a_0$

$x := 1$

power $:= 5 \bmod 7 = 5$

$i=0$ $a_0 = 1 \Rightarrow x := (1 \cdot 5) \bmod 7 = 5$ } 2 multip.

power $:= (5 \times 5) \bmod 7 = 4$

$i=1$ $a_1 = 0$ $\longrightarrow$ power $:= (4\times4) \bmod 7 = 2$ $\to$ 1 mult.

$i=2$ $a_2 = 0$ $\longrightarrow$ power $:= (2\times2) \bmod 7 = 4$ $\to$ 1 mult.

$i=3$ $a_3 = 0$ $\longrightarrow$ power $:= (4\times4) \bmod 7 = 2$ $\to$ 1 mult.

$i=4$ $a_4 = 0$ $\longrightarrow$ power $:= (2\times2) \bmod 7 = 4$ $\to$ 1 mult.

$i=5$ $a_5 = 1$ $\to$ $x := (5\times 4) \bmod 7 = 6$ $\to$ 1 mult.

power $:= (4\times4) \bmod 7 = 2$ $\to$ 1 mult

8 multip.

7. (15 points)

Use mathematical induction to prove that 9 divides

$$n^3 + (n+1)^3 + (n+2)^3$$

whenever n is a positive integer.

Proof by induction:

- Base step $n=1$ $\quad 1^3 + (1+1)^3 + (n+2)^3 = 1+8+27 = 36$ is divisible by 9

- assume $k^3 + (k+1)^3 + (k+2)^3 = 9 \times m$

then $(k+1)^3 + (k+2)^3 + (k+3)^3 = 9 \times m - k^3 + (k+3)^3$

$= 9 \times m - k^3 + k^3 + 9k^2 + 27k + 27$

$= 9 \times (m + k^2 + 3k + 3)$

which means that $(k+1)^3 + (k+2)^3 + (k+3)^3$ is divisible by 9.

thus $n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9 $\forall n \geq 1$

9. (10 points) Select primes $p = 11$ and $q = 5$ and public key $e = 3$. This means $d = 27$, in case you want to check your work. Encode the message "UP" by translating the letters in UP into their numerical equivalents (remember, A$\leftrightarrow$ 00, B$\leftrightarrow$ 01, etc.), grouping the numbers in blocks of four, and then using the RSA algorithm to encode the message.

U $\Leftrightarrow$ 20 P $\Leftrightarrow$ 15 $\varphi = (p-1)(q-1) = 40$ $pq = n = 55$

$M = 2015^3 \bmod 55 \equiv 8181353375 \bmod 55 = 30$

Encode message

decode

$30^{27} \bmod 55 = 35$ primes too small!!

8. (10 points)

(a) Use the Euclidean algoritm to find gcd(7,52).

(b) Find a~~n~~ multiplication inverse of 7 modulo 52

a) $52 = 7 \times 7 + 3$

$7 = 3 \times 2 + 1$

$\gcd(7,52) = 1.$

b) $1 = 7 - 3 \times 2$

$= 7 - 2(52 - 7 \times 7)$

$1 = 15 \times 7 - 2 \times 52$

so a multiplicative inverse of 7 modulo 52 is $\underline{\underline{15}}$