Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Information Technology
FH Zentralschweiz

Mathematical Basis - Exercise 1

Prof. Dr. Josef F. Bürgler

I.BA_IMATH, Semesterweek 01

Please write down to solution of the exercises in a consise but comprehensible way. Numerical results should be accurate to 4 digits. Sketches should be correct qualitatively. At least 75% of the exercises have to be solve satisfactorily. Due time is one week after we have discussed the corresponding topic in class.

1 Divisibility and Congruences

If a and b are integers and $a \neq 0$ then we say a divides b or b is divisible by a if there exists an integer k, s.t. $b = ak$. This is equivalent to $b \equiv 0 \mod a$, i.e. b is congruent to 0 modulo a.
We can therefore say: b is divisible by $a \neq 0$, or $a \neq 0$ divides b if and only if b is congruent to 0 modulo a.
Let's try some examples:

- 12 is divisible by 4, or 4 divides 12 because 12 is congruent to 0 modulo 4 ($12 \equiv 0 \mod 4$).
- 11 is not divisible by 3, or 3 does not divide 11 because 11 is not congruent to 0 modulo 3. In fact $11 \equiv 2 \mod 3$.
- 111111 is divisible by 3, or 3 divides 111111 because $111111 \equiv 0 \mod 3$. The trick here is to use the sum of the digits $1+1+1+1+1+1 = 6$. If the sum of the digits of n is divisible by 3 then n is divisble by 3. This rule and other rules of divisibility shall be investigated in this exercise!

The following rules hold (and we will prove some of them later on):

1. n is divisible by 2 if n is even, i.e. the last digit of n is divisible by 2, that is if the last digit of n is 0, 2, 4, 6, 8. This rule is obvious!
2. n is divisible by 3 if the sum of the digits in n is divisible by 3.
3. n is divisible by 4 if the number composed of the last two digits of n is divisible by 4. An example is 1024; here 24 is divisible by 4 and in fact $1024 = 4 \cdot 256$.

4. n is divisible by 5 if the last digit is either 0 or 5. This rule is easy and well known!
5. n is divisible by 6 if rules (1) and (2) hold, i.e. if n is divisible by 2 and 3.
6. n is divisible by 7 if ... (let's talk about this case in the end)
7. n is divisible by 8 ($8 \mid n$) if the number composed of the last three digits of n is divisible by 8. An example is $123'912$; here 912 is divisible by 8 ($912 = 8 \cdot 113$) and in fact $123'912 = 8 \cdot 15'489$.
8. n is divisible by 9 ($9 \mid n$) if the sum of the digits of n is divisible by 9 (we have learned that at school, right).
9. n is divisible by 10 ($10 \mid n$) if the last digit is 0. This is easy and obvious!
10. n is divisible by 11 ($11 \mid n$) if the alternating sum of the digits of n is divisible by 11 (we have learned this rule also at school, haven't we?)

Let's now prove two of the rules: divisibility by 8 and 11.

Proof. **Divisibility of n by 8:** We write n in the following form

$$n = d_m 10^m + d_{m-1} 10^{m-1} + \cdots + d_3 10^3 + d_2 10^2 + d_1 10 + d_0,$$

where $0 \leq d_i \leq 9$ for $i = 1, 2, \ldots, m$ and $d_m \neq 0$.
Example

$$123'912 = 1 \cdot 10^5 + 2 \cdot 10^4 + 3 \cdot 10^3 + 9 \cdot 10^2 + 1 \cdot 10 + 2,$$

where here $m = 5$, $d_5 = 1$, $d_4 = 2$, $d_3 = 3$, $d_2 = 9$, $d_1 = 1$, and $d_0 = 2$.
If we look at congruence of n modulo 8 we have

$$\begin{aligned} n &= d_m 10^m + d_{m-1} 10^{m-1} + \cdots + d_3 10^3 + d_2 10^2 + d_1 10 + d_0 \\ &= 10^3 \left(d_m 10^m + d_{m-1} 10^{m-1} + \cdots + d_3 \right) + \left(d_2 10^2 + d_1 10 + d_2 \right) \\ &\equiv \left(d_2 10^2 + d_1 10 + d_2 \right) \bmod 8. \end{aligned}$$

because $10^3 \equiv 0 \bmod 8$. If the number composed of the last three digits of n, i.e. $d_2 10^2 + d_1 10 + d_2$ is divisible by 8, then $n \equiv 0 \bmod 8$ which proves, that n is divisible by 8.

Divisibility of n by 11: Here we use the simple fact that $10 = 11 - 1$ and write n in the following form

$$\begin{aligned} n &= d_m 10^m + d_{m-1} 10^{m-1} + \cdots + d_3 10^3 + d_2 10^2 + d_1 10 + d_0 \\ &= d_m (11-1)^m + d_{m-1} (11-1)^{m-1} + \cdots + d_3 (11-1)^3 + d_2 (11-1)^2 + d_1 (11-1) + d_0 \end{aligned}$$

Now we have

$$\begin{aligned}
d_0 \bmod 11 &= d_0 \\
d_1(11-1) \bmod 11 &= -d_1 \\
d_2(11-1)^2 \bmod 11 &= d_2(11^2 - 2\cdot 11 + 1) \bmod 11 = d_2 \\
d_3(11-1)^3 \bmod 11 &= d_3(11^3 - 3\cdot 11^2 + 3\cdot 11 - 1) \bmod 11 = -d_3 \\
&\vdots \\
d_{m-1}(11-1)^{m-1} \bmod 11 &= d_{m-1}\sum_{j=0}^{m-1}\binom{m-1}{j}11^{m-1-j}(-1)^j \bmod 11 = (-1)^{m-1}d_{m-1} \\
d_m(11-1)^m \bmod 11 &= d_m\sum_{j=0}^{m}\binom{m}{j}11^{m-j}(-1)^j \bmod 11 = (-1)^m d_m
\end{aligned}$$

Here we have used the binomial theorem in the form

$$(11-1)^p = \sum_{j=0}^{p}\binom{p}{j}11^{p-j}(-1)^j = \binom{p}{0}11^p - \binom{p}{1}11^{p-1} + \binom{p}{2}11^{p-2} - \cdot + \cdots + (-1)^p\binom{p}{p}$$

In this expression all terms except the last are multiples of 11 and therefore divisible by 11 and hence

$$(11-1)^p \bmod 11 = (-1)^p.$$

This proves that

$$n \bmod 11 = d_m - d_{m-1} + \cdots + (-1)^{m-3}d_3 + (-1)^{m-2}d_2 + (-1)^{m-1}d_1 + (-1)^m d_0 \bmod 11$$

and therefore $11 \mid n$, i.e. n is divisible by 11, if the alternating sum of the digits of n is divisible by 11. □

Your Task: As an exercise You should prove that n is divisible by 9, i.e.$9 \mid n$, if the sum of the digits of n is divisible by 9. Hint: use the identity $10 = 9 + 1$.

2 Divisibility

Do there exist integers x, y, and z such that $6x + 9y + 15z = 107$? Hint: what are the divisors of the right hand and the left hand side of this equation?

3 Computing the (multiplicative) inverse I

The multiplicative inverse of a modulo n exists iff (if and only if) $\gcd(a,n) = 1$. If this is the case, it can be computed using the extended GCD algorithm. This amounts to find x and y s.t. (such that)

$$ax + ny = \gcd(a,n) = 1.$$

As an example with $n = 47$ and $a = 12$ we have

$$12 \cdot 4 + 47 \cdot (-1) = \gcd(12,47) = 1.$$

If take both sides of this equation modulo 47, we get

$$\begin{aligned} (12 \cdot 4 + 47 \cdot (-1)) \bmod 47 &= 1, \\ (12 \cdot 4) \bmod 47 &= 1, \end{aligned}$$

This tells us, that 4 is the (multiplicative) inverse of 12 modulo 47. In fact $12 \cdot 4 \mod 47 = 48 \mod 47 = 1$.

Your Task: Find the multiplicative inverses of a modulo n (if it exists) if

1. $n = 13$, $a = 5$,
2. $n = 15$, $a = 7$.
3. $n = 15$, $a = 5$.

If n is small, it is sometimes faster to guess the inverse!

4 Computing the (multiplicative) inverse II

Which of the elements in $\mathbb{Z}_6$ do have a (multiplicative) inverse modulo 6? For each of these elements compute the inverse and prove, that it is indeed the inverse by computing $a \cdot a^{-1} \bmod 6$.

5 Computing the (multiplicative) inverse III

The multiplicative inverse of a modulo n can be computed

- by guessing which works well if n is small
- by writing down the multiplication table; which also only works when n is small,
- by advocating the extended GCD

- with the help of Fermat's little theorem

Your Task: Compute the multiplicative inverse of 9 modulo 11 by using all of the four methods.

6 Fermat's little theorem

It states, that for any prime p which is not a divisor of a the following holds

$$a^{p-1} \equiv 1 \bmod p \quad \text{i.e.} \quad a^{p-1} \equiv_p 1. \tag{1}$$

Based on this theorem is a test for primality of a number. Suppose that the primality of an integer n is not known. If we can find an integer a, that is relatively prime (coprime) to n, i.e. $\gcd(a,n) = 1$, such that $a^{n-1} \not\equiv 1 \pmod{n}$, then we have conclusive proof that n is composite (not prime). Such a number a is said to be a Fermat witness for the compositeness (non-primality) of n. If a Fermat witness is found, the number being tested is proved to be composite. If the congruence relation (1) is true for n and a, then n is said to be a probable prime to base a. Furthermore, if n happens to be a composite number, then n is said to be a pseudoprime to base a. A pseudoprime is a composite number that possesses the prime-like proberty (1) for one base a.
If (1) holds for several (or all) bases a, then the number n is found to be probable prime and therefore likely a prime number. There are composite numbers (like the carmicel numbers) which pass (1) for every a, but are not primes!
Here the Fermat primality test in python:

```
from random import randint

def Fermat_isProbablyPrime(n,k = 5):
    if (n < 2 ):
        return False
    output = True
    for i in range(0, min(n,k)):
        a = randint(1, n-1)
        if (pow(a, n-1, n) != 1):
            return False
    return output
```

we can call this functions as follows to find the probable primes smaller than 100:

```
max = 100

for n in range(2,max):
    if Fermat_isProbablyPrime(n,10):
        print("n = %d is prime" % n)
```

Have fun with crypto!