INF1003 Tutorial 2

Name: Timothy Chia **Topic:** Number Theory
Student ID: 2501530 **Due Date:** 14th September 2025, 10:00 PM

1. Evaluate the following:

(a) 13 mod 3.

Solution. We divide 13 by 3:

$$13 = 3 \cdot 4 + 1.$$

The remainder is 1, so

$$13 \bmod 3 = 1.$$

(b) -22 mod 23.

Solution. We want the remainder in the range $0 \le r \le 22$.

Note that

$$-22 + 23 = 1,$$

so -22 and 1 differ by a multiple of 23:

$$-22 \equiv 1 \pmod{23}.$$

Therefore

$$-22 \bmod 23 = 1.$$

2. Find the integer a such that

$$a \equiv -15 \pmod{27} \quad \text{and} \quad 0 \le a \le 26.$$

Solution. We add 27 to -15 to obtain an equivalent non-negative representative:

$$-15 + 27 = 12.$$

Hence

$$-15 \equiv 12 \pmod{27},$$

so the required integer is

$$a = 12.$$

3. Decide whether 80 and/or 103 are congruent to $5 \pmod{17}$.

Solution. Compute each number modulo 17.

For 80:

$$80 = 17 \cdot 4 + 12 \quad \Rightarrow \quad 80 \equiv 12 \pmod{17}.$$

For 103:

$$103 = 17 \cdot 6 + 1 \quad \Rightarrow \quad 103 \equiv 1 \pmod{17}.$$

We compare with 5:

$$12 \not\equiv 5 \pmod{17}, \qquad 1 \not\equiv 5 \pmod{17}.$$

Therefore, neither 80 nor 103 is congruent to $5 \pmod{17}$.

4. Compute

$$(-133 \bmod 23) + (26 \bmod 23).$$

Solution. First find each remainder separately.

For $-133 \bmod 23$:

$$23 \cdot 6 = 138, \quad -133 + 138 = 5,$$

so

$$-133 \equiv 5 \pmod{23} \quad \Rightarrow \quad -133 \bmod 23 = 5.$$

For $26 \bmod 23$:

$$26 = 23 \cdot 1 + 3 \quad \Rightarrow \quad 26 \bmod 23 = 3.$$

Add the two remainders:

$$(-133 \bmod 23) + (26 \bmod 23) = 5 + 3 = 8.$$

So the value of the expression is

$$8.$$

5. Compute

$$(89^3 \bmod 74)^4 \bmod 26.$$

Solution. Step 1: Compute $89^3 \bmod 74$.

First reduce 89 modulo 74:

$$89 = 74 + 15 \quad \Rightarrow \quad 89 \equiv 15 \pmod{74}.$$

Then

$$89^2 \equiv 15^2 = 225 \pmod{74}.$$

Now reduce 225 modulo 74:

$$74 \cdot 3 = 222, \quad 225 - 222 = 3,$$

so

$$89^2 \equiv 3 \pmod{74}.$$

Next,

$$89^3 \equiv 89^2 \cdot 89 \equiv 3 \cdot 15 = 45 \pmod{74}.$$

Thus

$$89^3 \bmod 74 = 45.$$

Step 2: Compute $45^4 \bmod 26$.

First reduce 45 modulo 26:

$$45 = 26 + 19 \quad \Rightarrow \quad 45 \equiv 19 \pmod{26}.$$

So

$$45^4 \equiv 19^4 \pmod{26}.$$

Compute 19^2 modulo 26:

$$19^2 = 361, \quad 26 \cdot 13 = 338, \quad 361 - 338 = 23,$$

so

$$19^2 \equiv 23 \pmod{26}.$$

Then

$$19^4 = (19^2)^2 \equiv 23^2 = 529 \pmod{26}.$$

Now reduce 529 modulo 26:

$$26 \cdot 20 = 520, \quad 529 - 520 = 9,$$

so

$$19^4 \equiv 9 \pmod{26}.$$

Therefore

$$(89^3 \bmod 74)^4 \bmod 26 = 9.$$

6. Determine whether each of these integers is prime.

(a) 97

(b) 111

(c) 187

Solution.

(a) 97.

We check divisibility by primes up to $\sqrt{97} \approx 9.8$, i.e. $2, 3, 5, 7$.

- 97 is odd, so not divisible by 2.
- Sum of digits is $9 + 7 = 16$, not a multiple of 3, so not divisible by 3.
- It does not end with 0 or 5, so not divisible by 5.
- $97/7 = 13$ remainder 6, so not divisible by 7.

Since there is no prime divisor $\leq \sqrt{97}$, 97 is prime.

(b) 111.

Sum of digits: $1 + 1 + 1 = 3$, which is divisible by 3, hence

$$111 \text{ is divisible by } 3.$$

Indeed

$$111 = 3 \cdot 37.$$

Therefore 111 is not prime.

(c) 187.

We test small primes:

- 187 is odd, so not divisible by 2.
- Sum of digits is $1 + 8 + 7 = 16$, not divisible by 3.
- It does not end with 0 or 5, so not divisible by 5.

Try dividing by 11:

$$11 \cdot 17 = 187.$$

So $187 = 11 \cdot 17$, and hence is not prime.

7. Find the prime factorisation of 1001 and 1111.

Solution.

For 1001:

$$1001 = 7 \cdot 143, \quad 143 = 11 \cdot 13.$$

Therefore

$$1001 = 7 \cdot 11 \cdot 13.$$

For 1111:

First note that 1111 ends with 1, so it is not divisible by 2 or 5. Check divisibility by 11:

$$1111/11 = 101,$$

so

$$1111 = 11 \cdot 101.$$

Since 101 is prime, this is the prime factorisation.

8. Determine whether the integers in each of these sets are pairwise relatively prime.

(a) $11, 15, 19$

(b) $12, 17, 31, 37$

Solution.

A set of integers is *pairwise relatively prime* if the gcd of every pair of distinct integers in the set is 1.

(a) $11, 15, 19$.

Factor each number:

$$11 = 11, \quad 15 = 3 \cdot 5, \quad 19 = 19.$$

The prime factors are:

$$11 : \{11\}, \quad 15 : \{3, 5\}, \quad 19 : \{19\}.$$

No prime factor is shared between any two numbers, so

$$\gcd(11, 15) = 1, \quad \gcd(11, 19) = 1, \quad \gcd(15, 19) = 1.$$

Hence the set is pairwise relatively prime.

(b) $12, 17, 31, 37$.

Factor each number:

$$12 = 2^2 \cdot 3, \quad 17, 31, 37 \text{ are prime.}$$

The primes $17, 31, 37$ are all distinct and none of them divides 12. Therefore every pair from $\{12, 17, 31, 37\}$ has gcd 1, so this set is also pairwise relatively prime.

9. What are the greatest common divisors of each of these pairs of integers?

(a) $\left(3^7 \cdot 5^3 \cdot 7^3\right)$ and $\left(2^{11} \cdot 3^5 \cdot 5^9 \cdot 7^3\right)$.

(b) $(11 \cdot 13 \cdot 17)$ and $\left(2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3\right)$.

(c) $(41 \cdot 43 \cdot 53)$ and $(41 \cdot 43 \cdot 53)$.

(d) $\left(3^{13} \cdot 5^{17}\right)$ and $\left(2^{12} \cdot 7^{21}\right)$.

Solution.

Recall: if

$$a = \prod p_i^{\alpha_i}, \quad b = \prod p_i^{\beta_i}$$

are prime factorisations over the same set of primes p_i, then

$$\gcd(a, b) = \prod p_i^{\min(\alpha_i, \beta_i)}.$$

(a)

$$a = 3^7 \cdot 5^3 \cdot 7^3, \quad b = 2^{11} \cdot 3^5 \cdot 5^9 \cdot 7^3.$$

Take the minimum exponents for each prime present in both:

$$\gcd(a, b) = 3^{\min(7,5)} \cdot 5^{\min(3,9)} \cdot 7^{\min(3,3)} = 3^5 \cdot 5^3 \cdot 7^3.$$

Numerically,

$$3^5 \cdot 5^3 \cdot 7^3 = 10{,}418{,}625.$$

(b)

$$a = 11 \cdot 13 \cdot 17, \quad b = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3.$$

The primes in a are $11, 13, 17$, while the primes in b are $2, 3, 5, 7$. There is no common prime factor, so

$$\gcd(a, b) = 1.$$

(c)

$$a = 41 \cdot 43 \cdot 53, \quad b = 41 \cdot 43 \cdot 53.$$

Here a and b are the same number, so

$$\gcd(a, b) = 41 \cdot 43 \cdot 53.$$

(Numerically, this is 93,439.)

(d)

$$a = 3^{13} \cdot 5^{17}, \quad b = 2^{12} \cdot 7^{21}.$$

The primes in a are 3 and 5; the primes in b are 2 and 7. There is no overlap, so

$$\gcd(a, b) = 1.$$

10. Find gcd(1000, 625) and lcm(1000, 625) and verify that

$$\gcd(1000, 625) \cdot \operatorname{lcm}(1000, 625) = 1000 \cdot 625.$$

Solution.

First find the prime factorisations:

$$1000 = 10^3 = (2 \cdot 5)^3 = 2^3 \cdot 5^3, \qquad 625 = 5^4.$$

The gcd takes the minimum power of each prime:

$$\gcd(1000, 625) = 2^{\min(3,0)} \cdot 5^{\min(3,4)} = 2^0 \cdot 5^3 = 125.$$

The lcm takes the maximum power of each prime:

$$\operatorname{lcm}(1000, 625) = 2^{\max(3,0)} \cdot 5^{\max(3,4)} = 2^3 \cdot 5^4 = 8 \cdot 625 = 5000.$$

Now verify the product identity:

$$\gcd(1000, 625) \cdot \operatorname{lcm}(1000, 625) = 125 \cdot 5000 = 625{,}000,$$

and

$$1000 \cdot 625 = 625{,}000.$$

So the equality holds.

11. Use the Euclidean algorithm to find:

(a) gcd(111, 201);

(b) gcd(1001, 1331);

(c) gcd(1000, 5040).

Solution.

(a) gcd(111, 201).

Apply the Euclidean algorithm:

$$201 = 1 \cdot 111 + 90,$$

$$111 = 1 \cdot 90 + 21,$$

$$90 = 4 \cdot 21 + 6,$$

$$21 = 3 \cdot 6 + 3,$$

$$6 = 2 \cdot 3 + 0.$$

The last non-zero remainder is 3, so

$$\gcd(111, 201) = 3.$$

(b) $\gcd(1001, 1331)$.

$$1331 = 1 \cdot 1001 + 330,$$
$$1001 = 3 \cdot 330 + 11,$$
$$330 = 30 \cdot 11 + 0.$$

The last non-zero remainder is 11, so

$$\gcd(1001, 1331) = 11.$$

(c) $\gcd(1000, 5040)$.

$$5040 = 5 \cdot 1000 + 40,$$
$$1000 = 25 \cdot 40 + 0.$$

The last non-zero remainder is 40, so

$$\gcd(1000, 5040) = 40.$$

12. Express the greatest common divisor of each of these pairs of integers a, b as

$$sa + tb$$

for some integers s and t.

(a) $117, 213$

(b) $3454, 4666$

Solution.

(a) $a = 117,\ b = 213$.

From the Euclidean algorithm:

$$213 = 1 \cdot 117 + 96,$$
$$117 = 1 \cdot 96 + 21,$$
$$96 = 4 \cdot 21 + 12,$$
$$21 = 1 \cdot 12 + 9,$$
$$12 = 1 \cdot 9 + 3,$$
$$9 = 3 \cdot 3 + 0.$$

Thus $\gcd(117, 213) = 3$.

Now work backwards to express 3 in terms of 117 and 213.

From $12 = 9 + 3$ we get

$$3 = 12 - 9.$$

From $21 = 12 + 9$ we get $9 = 21 - 12$, so

$$3 = 12 - (21 - 12) = 2 \cdot 12 - 21.$$

From $96 = 4 \cdot 21 + 12$ we get $12 = 96 - 4 \cdot 21$, hence

$$3 = 2(96 - 4 \cdot 21) - 21 = 2 \cdot 96 - 9 \cdot 21.$$

From $117 = 96 + 21$ we get $21 = 117 - 96$, so

$$3 = 2 \cdot 96 - 9(117 - 96) = 11 \cdot 96 - 9 \cdot 117.$$

From $213 = 117 + 96$ we get $96 = 213 - 117$, giving

$$3 = 11(213 - 117) - 9 \cdot 117 = 11 \cdot 213 - 20 \cdot 117.$$

Thus

$$3 = (-20) \cdot 117 + 11 \cdot 213,$$

so we can take

$$s = -20, \quad t = 11.$$

(b) $a = 3454,\ b = 4666.$

First use the Euclidean algorithm to find the gcd:

$$4666 = 1 \cdot 3454 + 1212,$$

$$\begin{aligned}
3454 &= 2 \cdot 1212 + 1030, \\
1212 &= 1 \cdot 1030 + 182, \\
1030 &= 5 \cdot 182 + 120, \\
182 &= 1 \cdot 120 + 62, \\
120 &= 1 \cdot 62 + 58, \\
62 &= 1 \cdot 58 + 4, \\
58 &= 14 \cdot 4 + 2, \\
4 &= 2 \cdot 2 + 0.
\end{aligned}$$

So $\gcd(3454, 4666) = 2$.

Now work backwards to express 2 as a linear combination of 3454 and 4666.

From $58 = 14 \cdot 4 + 2$ we have

$$2 = 58 - 14 \cdot 4.$$

From $62 = 58 + 4$ we have $4 = 62 - 58$, hence

$$2 = 58 - 14(62 - 58) = 15 \cdot 58 - 14 \cdot 62.$$

From $120 = 62 + 58$ we have $58 = 120 - 62$, so

$$2 = 15(120 - 62) - 14 \cdot 62 = 15 \cdot 120 - 29 \cdot 62.$$

From $182 = 120 + 62$ we have $62 = 182 - 120$, hence

$$2 = 15 \cdot 120 - 29(182 - 120) = 44 \cdot 120 - 29 \cdot 182.$$

From $1030 = 5 \cdot 182 + 120$ we have $120 = 1030 - 5 \cdot 182$, giving

$$2 = 44(1030 - 5 \cdot 182) - 29 \cdot 182 = 44 \cdot 1030 - 249 \cdot 182.$$

From $1212 = 1030 + 182$ we have $182 = 1212 - 1030$, so

$$2 = 44 \cdot 1030 - 249(1212 - 1030) = 293 \cdot 1030 - 249 \cdot 1212.$$

From $3454 = 2 \cdot 1212 + 1030$ we have $1030 = 3454 - 2 \cdot 1212$, hence

$$2 = 293(3454 - 2 \cdot 1212) - 249 \cdot 1212 = 293 \cdot 3454 - 835 \cdot 1212.$$

Finally, from $4666 = 3454 + 1212$ we have $1212 = 4666 - 3454$, so

$$2 = 293 \cdot 3454 - 835(4666 - 3454) = (293 + 835) \cdot 3454 - 835 \cdot 4666 = 1128 \cdot 3454 - 835 \cdot 4666.$$

Thus

$$2 = 1128 \cdot 3454 + (-835) \cdot 4666,$$

so we can take

$$s = 1128, \quad t = -835.$$