> *Mathematics is the queen of the sciences and number theory is the queen of mathematics. (Die Mathematik ist die Königin der Wissenschaften und die Zahlentheorie ist die Königin der Mathematik.).* - Carl Friedrich Gauss

Question 1. Show that n and $n+1$ are coprime for all $n \geq 1$.

Solution:
If e is an integer that divides n and $n+1$ simultaneously, then e also divides $(n+1)-n = 1$. Thus $e = \pm 1$. Hence the gcd of n and $n+1$ must be 1.

Question 2. Show that if e divides a and b then e divides $ar + bs$ for any integers r and s.

Solution:
Suppose e divides a and b. Then $a = ke$ and $b = je$ for some integers k and j. Thus:

$$ar + bs = ker + jes = e(kr + js)$$

and therefore e also divides $ar + bs$.

Question 3. Use Euclid's algorithm to find the following GCD's:
(a) $(121, 365)$,

(b) $(89, 144)$,

(c) $(295, 595)$,

(d) $(1001, 1309)$.

Solution:
Use Euclid's algorithm (ask me if you have doubts):

1. $(121, 365) = 1$,
2. $(89, 144) = 1$,
3. $(295, 595) = 5$,
4. $(1001, 1309) = 77$.

Question 4. Find the GCD of 17017 and 18900 using Euclid's algorithm.

Solution:
$(17017, 18900) = 7$, show your work!

Question 5. Find d, the GCD of a and b, i.e., $d = (a, b)$, and $r, s \in \mathbb{Z}$ such that $ar + bs = d$:
(a) $a = 267$ and $b = 112$,

(b) $a = 242$ and $b = 1870$.

Solution:
Use Euclid's and then backwards... show your work!

1. $(267, 112) = 1$, and $r = -13$ and $s = 31$, i.e. $267 \cdot (-13) + 112 \cdot (31) = 1$,
2. $(242, 1870) = 22$ and $r = 31$ and $s = -4$, i.e. $242 \cdot (31) + 1870 \cdot (-4) = 22$.

Question 6. Find all solutions with integer coefficients x and y:
(a) $267x + 112y = 3$,

(b) $376x + 72y = 18$.

Solution:

1. $267x + 112y = 3$.

   First, we find the GCD of 267 and 112 using Euclid's algorithm (show your work). It is equal to 1. Next, we find one solution to $267x + 112y = 1$ by going backwards. We find:
   $$267 \cdot (-13) + 112 \cdot (31) = 1$$
   Therefore, if we multiply throughout by 3 we get:
   $$267 \cdot (-39) + 112 \cdot (93) = 3.$$
   By a theorem in class (Theorem 2.9.4 in the book), all the solutions are:
   $$x = -39 + \frac{112}{1}n = -39 + 112n, \quad y = 93 - \frac{267}{1}n = 93 - 267n$$
   for all integers n, since $\gcd(112, 267) = 1$.

2. $376x + 72y = 18$.

   If you calculate the GCD of 376 and 72 you will find out that it is equal to 8. However, 8 does not divide 18. Hence, by a theorem in class (Prop. 2.9.1 in the book), this equation does not have solutions in x, y integers.

Question 7. Find all solutions with integer coefficients x and y:
(a) $203x + 119y = 47$, 48, or 50,

(b) $203x + 119y = 49$.

Solution:

1. $203x + 119y = 47, 48, 50$.

   These equations do not have solutions because the GCD of 203 and 119 is equal to 7 and 7 does not divide any of 47, 48 or 50 (by Prop. 2.9.1).

2. $203x + 119y = 49$.

   First we use Euclid's algorithm to find a solution of $203x + 119y = 1$, which can be done because the GCD of 203 and 119 is equal to 1. (Show your work) We find that:

$$203 \cdot (-7) + 119 \cdot (12) = 7$$

   Now multiply the equation by 7 to obtain:

$$203 \cdot (-49) + 119 \cdot (84) = 49$$

   Therefore, all the solutions are given by:

$$x = -49 + \frac{119}{7}n = -49 + 17n, \quad y = 84 - \frac{203}{7}n = 84 - 29n,$$

   by Theorem 2.9.4, where we have used the fact that the GCD is 7. Of all these, the smallest is $x = 2$ and $y = -3$.

Question 8. Prove that if $(a, b) = d$ then $(\frac{a}{d}, \frac{b}{d}) = 1$.

Solution:
Let $(a, b) = d$. Then, by Bezout's identity, there are r, s integers such that

$$ar + bs = d.$$

Since d divides a and b, we may divide and get:

$$\frac{a}{d}r + \frac{b}{d}s = 1.$$

Therefore, by Bezout's identity, the GCD of $\frac{a}{d}$ and $\frac{b}{d}$ must divide 1 and it is thus equal to 1.

Question 9. Find all the natural, integral and rational roots of the polynomial equation

$$5x^3 + 27x^2 - 153x + 81 = 0.$$

Solution:
In order to find any rational solutions of this equation, we use the theorem that says that if $\frac{m}{n}$ is a root, then m is a divisor of 81 and n is a divisor of 5. Thus, $m \in \{\pm 1, \pm 3, \pm 9, \pm 27, \pm 81\}$, and $n \in \{1, 5\}$. After checking these possibilities, we find that $x = 3 \in \mathbb{N}$, $x = -9 \in \mathbb{Z}$ and $x = \frac{3}{5}$ are all the roots of the equation.

Question 10. Show that if $n > 1$ is not prime then n has a prime divisor $\leq \sqrt{n}$.

Solution:
Let n be composite and suppose for a contradiction that every prime divisor of n is bigger than $\sqrt{n}$. Since n is composite, $n = ab$ for some $1 < a, b < n$. Since every integer has a prime divisor, and since every prime divisor of a or b is also a divisor of n, we conclude that $a, b > \sqrt{n}$. But then:

$$n = ab > \sqrt{n}\sqrt{n} = n$$

Hence $n > n$ which is a clear contradiction. So there must be at least one prime divisor $\leq \sqrt{n}$.

Question 11. Is 44497 prime? Why, or why not?

Solution:
Yes it is prime. In order to check this, one needs to check that all primes between 1 and $\sqrt{44497} = 210.9...$ do not divide 44497. (Show some work, at least a list of primes between 1 and 210).

Question 12.
(a) Prove that a natural number is a square if and only if the exponent of each prime factor is even.

(b) Prove that if a number n is not a square then $\sqrt{n}$ is irrational.

Solution:

1. Suppose n is a square. Then $n = b^2$ for some integer b. By the FTA, b has a prime factorization
$$b = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$
where all the p_i are distinct primes and $e_i > 0$. Hence:
$$n = b^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}$$
and this is the prime factorization of n, with all even exponents.
Conversely, if
$$n = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}$$
then $n = b^2$ with
$$b = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$
and so n is a square.

2. Suppose n is not a square. Then there exists a prime p that divides n and in the prime factorization of n, the prime p appears to an odd power. Thus $n = p^{2e+1}m$ for some $e \geq 0$ and some m relatively prime to p (why?). Suppose that $\sqrt{n} = \frac{s}{t}$ for some integers s, t. Then
$$nt^2 = s^2$$
and therefore $p^{2e+1}mt^2 = s^2$. However, s^2 is clearly a square, so the exponents in its prime factorization must be all even, but on the left hand side, p appears to an odd power (notice that even if a p appears in t, it would only add an even amount to $2e+1$ leaving the exponent odd). This is a contradiction, and $\sqrt{n}$ must be irrational.

Question 13. Show that $100^{(1/3)}$ is irrational.

Solution:
Suppose that $100^{(1/3)} = \frac{n}{m}$ for some integers n, m. Then $100m^3 = n^3$ or equivalently:

$$2^2 \cdot 5^2 \cdot m^3 = n^3.$$

By the fundamental theorem of arithmetic, m and n have unique factorizations as products of prime numbers. Let 5^e and 5^f be the powers of 5 that appears in the factorization of m and n respectively (with $e \geq 0$ and $f \geq 0$). By the uniqueness of the factorization, the power of 5 that appears in the factorization of the left hand side is of the form $2+3e$ while on the right hand side is of the form $3f$, and they must be equal. But $2+3e = 3f$ has no solutions in integers e, f, because it would imply that $2 = 3e + 3f = 3(e+f)$ and so 2 is a multiple of 3. This is a contradiction.

Question 14. Show that if a, b are natural numbers with $(a, b) = 1$ and ab is a square, then a and b are also squares.

Solution:
We use Question 12. Since ab is a square, we have

$$ab = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}$$

where all the p_i are distinct primes and $e_i > 0$. Since a and b are relatively prime, if p_i divides a then it does not divide b. Thus, after reordering the primes p_i, we may assume WLOG that:

$$a = p_1^{2e_1} p_2^{2e_2} \cdots p_i^{2e_i}, \quad b = p_{i+1}^{2e_{i+1}} p_{i+2}^{2e_{i+2}} \cdots p_r^{2e_r}$$

And so, the exponents of the primes in the factorizations of a and b are all even. Hence, by Question 12, a and b are also squares.