INF 240 - Exercise problems - 4
Solutions

Nikolay Kaleyski

Exercise 1.

- *To find* $\gcd(115, 69)$*: divide* 115 *by* 69 *with remainder, i.e. find a quotient* q *and a remainder* $r < 69$ *such that* $115 = 69q + r$*. This is clearly*

$$115 = 69 \cdot 1 + 46.$$

  Since the remainder $r = 46$ *is not zero, we repeat the above step with* 69 *and* 46 *in place of* 115 *and* 69*:*

$$69 = 46 \cdot 1 + 23.$$

  The remainder $r = 23$ *is still not zero, so we divide again:*

$$46 = 23 \cdot 2 + 0.$$

  This time, the remainder is zero, so we terminate; the last non-zero remainder is the greatest common divisor of the two input integers, i.e. $\gcd(115, 69) = 23$.

- *To find* α *and* β *such that* $115\alpha + 69\beta = \gcd(115, 69) = 23$*: beginning with the last equation with a non-zero remainder (which is equal to* $\gcd(115, 69)$*), as a combination of the other two integers involved in the equation:*

$$23 = 69 - 46.$$

  From the very first equation, we can express 46 *as a combination of* 115 *and* 69 *as* $46 = 115 - 69$*. We now substitute this into the above equation and simplify in order to obtain*

$$23 = 69 - (115 - 69) = -115 + 2 \cdot 69.$$

  Thus $\alpha = -1$ *and* $\beta = 2$ *satisfy* $115\alpha + 69\beta = 23$.

- *To find* $\gcd(115, 48)$*: divide* 115 *by* 48 *to get*

$$115 = 48 \cdot 2 + 19.$$

  Repeat:

$$48 = 19 \cdot 2 + 10.$$

Repeat:

$$19 = 10 \cdot 1 + 9.$$

Repeat:

$$10 = 9 \cdot 1 + 1.$$

Repeat:

$$9 = 1 \cdot 9 + 0.$$

Having obtained a zero remainder, we terminate, and see that $\gcd(115, 48) = 1$ *since* 1 *is the last non-zero remainder that we obtained.*

- *To find* α *and* β *satisfying* $115\alpha + 48\beta = 1$*: we first write*

$$1 = 10 - 9$$

from the last equation with a non-zero remainder. We thus have an expression of 1 *as a combination of* 9 *and* 10*. But from the next-to-last equation with a non-zero remainder, we can express* 9 *as* $9 = 19 - 10$ *and substitute this into the above equation to obtain*

$$1 = 10 - (19 - 10) = 2 \cdot 10 - 19.$$

We go one equation up, and see that we can express 10 *as* $10 = 48 - 2 \cdot 19$*. We substitute this above to get*

$$1 = 2(48 - 2 \cdot 19) - 19 = 2 \cdot 48 - 5 \cdot 19.$$

Finally, from the very first equation, we have $19 = 115 - 2 \cdot 48$ *so that the above becomes*

$$1 = 2 \cdot 48 - 5(115 - 2 \cdot 48) = -5 \cdot 115 + 12 \cdot 48.$$

Exercise 2. *To find the least common multiples, we use the results from the previous exercise and the formula*

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

So we have

$$\operatorname{lcm}(115, 69) = \frac{115 \cdot 69}{\gcd(115, 69)} = \frac{115 \cdot 69}{23} = 345$$

and

$$\operatorname{lcm}(115, 48) = \frac{115 \cdot 48}{\gcd(115, 48)} = \frac{115 \cdot 48}{1} = 115 \cdot 48 = 5520.$$

Exercise 3. *To find the greatest common divisor of* $f(x) = x^5 + 2x^4 - x^2 + 1$ *and* $g(x) = x^4 - 1$*, we apply the same procedure as in the case of integers: we divide* $f(x)$ *by* $g(x)$ *with remainder, i.e. we find a quotient* $q(x)$ *and a remainder* $r(x)$ *such that* $f(x) = g(x)q(x) + r(x)$*. In the first step, we obtain*

$$f(x) = g(x)(x + 2) + (-x^2 + x + 3).$$

Since the remainder $r(x) = (-x^2 + x + 3)$ is non-zero, we divide $g(x)$ by $r(x)$ in the next step:

$$g(x) = (-x^2 + x + 3)(-x^2 - x - 4) + (7x + 11).$$

Once again, the remainder is non-zero, so we divide $(-x^2 + x + 3)$ by $(7x + 11)$:

$$(-x^2 + x + 3) = (7x + 11)(-\frac{1}{7}x + \frac{18}{49}) - \frac{51}{49}.$$

Although the remainder here is not zero, it is a constant, and it is clear that in the next step we will be dividing a polynomial by a constant, which can always be done with zero remainder. Hence this is the last step in the computation, and the greatest common divisor of $f(x)$ and $g(x)$ is the last non-zero remainder, which in this case is the constant polynomial $-\frac{51}{49}$. We have to remember to "normalize" the polynomial so that it is monic, and we do this by dividing it by the coefficient in front of its highest power of x (the so-called leading coefficient). In this case, the leading coefficient is $-\frac{51}{49}$, and dividing by it yields 1; thus $\gcd(f(x), g(x)) = 1$, *i.e. $f(x)$ and $g(x)$ are co-prime.*

Exercise 4. *To find the least common multiple of $f(x)$ and $g(x)$ from the previous exercise, we once again make use of the formula*

$$\gcd(f(x), g(x)) \cdot \operatorname{lcm}(f(x), g(x)) = f(x) \cdot g(x)$$

which holds for any two polynomials $f(x)$ and $g(x)$. In our case, we get

$$\operatorname{lcm}(f(x), g(x)) = \frac{f(x) \cdot g(x)}{\gcd(f(x), g(x))} = \frac{(x^5 + 2x^4 - x^2 + 1)(x^4 - 1)}{1} = x^9 + 2x^8 - x^6 - x^5 - x^4 + x^2 - 1.$$

Exercise 5. *To find the greatest common divisor of $f(x) = x^7 + 1$ and $g(x) = x^5 + x^3 + x + 1$, we once again apply the Euclidean algorithm. In this case, we remark that the only possible coefficients in $\mathbb{F}_2$ are 0 and 1, and that addition and subtraction are the same operation (since $-1 \equiv 1 \mod 2$) which greatly simplifies computation. In the first step, we have*

$$x^7 + 1 = (x^2 + x)(x^5 + x^3 + x + 1) + (x^2 + x).$$

The remainder, $x^2 + x$, is non-zero, and so we divide again:

$$x^5 + x^3 + x + 1 = (x^3)(x^2 + 1) + (x + 1).$$

And again:

$$x^2 + 1 = (x + 1)(x + 1) + 0.$$

This time, the remainder is zero, and $\gcd(f(x), g(x)) = (x + 1)$ *since the latter is the last non-zero remainder in the algorithm.*

Exercise 6. *As before, we use that* $\gcd(f(x), g(x)) \cdot \operatorname{lcm}(f(x), g(x)) = f(x) \cdot g(x)$, *so we get*

$$\operatorname{lcm}(f(x), g(x)) = \frac{f(x) \cdot g(x)}{\gcd(f(x), g(x))} = \frac{(x^7 + 1)(x^5 + x^3 + x + 1)}{x + 1} =$$
$$\frac{x^{12} + x^{10} + x^8 + x^7 + x^5 + x^3 + x + 1}{x + 1} = x^{11} + x^{10} + x^7 + x^4 + x^3 + 1.$$