Math 261 — Fall 2022
Number Theory

https://sites.aub.edu.lb/kmakdisi/

Problem set 2, due Friday, September 16 at the beginning of class

Exercise 2.1: Use the Euclidean algorithm to find the following GCDs:

$$\gcd(14784, 14853960), \qquad \gcd(93933, 99939), \qquad \gcd(10001, 100001).$$

(Note: just do the standard Euclidean algorithm and not the extended Euclidean algorithm; no need to express the GCD as a linear combination of the two numbers. In other words, just find the entries n_i in the first column, without finding the x_i and y_i in the second and third columns.)

Exercise 2.2: a) By considering the prime factorizations of a and b, show that the equation $a^2 = 2b^2$ does not have any solutions with $a, b \in \mathbf{Z}$, other than the trivial solution $a = b = 0$. Use this fact to show that $\sqrt{2} \notin \mathbf{Q}$.

b) More generally, let $n \in \mathbf{Z}$ with n not equal to the square of an integer. Show that $\sqrt{n} \notin \mathbf{Q}$. (If you are stuck, try to first show in scratch work the special case $\sqrt{2100} \notin \mathbf{Q}$. That should give you a feel for the general case.)

Exercise 2.3: Let $a, b \in \mathbf{Z}$ be **nonzero** integers. Suppose that ab is a square, i.e., there exists $y \in \mathbf{Z}$ such that $ab = y^2$.

a) If furthermore $\gcd(a, b) = 1$, then show that a is either a square, or the negative of a square (i.e., there exists $r \in \mathbf{Z}$ such that $a = r^2$ or $a = -r^2$).

b) If instead $\gcd(a, b) = p$ for a prime p, what can you say about a?

c) If $x, y \in \mathbf{Z}$ satisfy $y^2 = x^3 + px$ for a prime p, show that x is either a square or p times a square (so $x = \ell^2$ or $x = p\ell^2$ for some integer ℓ).

Exercise 2.4: a) Find all (integer) solutions of each of the following equations:

$$363x + 400y = 1, \qquad 87x + 105y = 0, \qquad 87x + 105y = 54.$$

b) Find all solutions of $10x + 14y + 35z = 103$. (Hint: $10x + 14y$ can equal any even number $2w$.)

c) Given a, b, c, show that the equation $ax + by + cz = m$ is solvable if and only if m is a multiple of the GCD (a, b, c). (Bonus: find all the solutions.)

d) Solve each of the following congruences (the first two should look familiar):

$$\begin{aligned} 363x &\equiv 1 \pmod{400}, & 87x &\equiv 54 \pmod{105}, \\ 29x &\equiv 18 \pmod{60}, & 28x &\equiv 18 \pmod{60}. \end{aligned}$$

Exercise 2.5: a) Let p be prime and let $a, b \in \mathbf{Z}$. Suppose that $\gcd(a, p^2) = p$ and $\gcd(b, p^3) = p^2$. Find $\gcd(ab, p^{10})$ and $\gcd(a + b, p^{10})$.

b) For p prime and $n \in \mathbf{Z}$, define

$$v_p(n) = \begin{cases} k, & \text{if } n = p^k \ell \text{ with } p \nmid \ell, \\ \text{"}\infty\text{"}, & \text{if } n = 0. \end{cases}$$

Show that for all a, b we have $v_p(ab) = v_p(a) + v_p(b)$ and $v_p(a + b) \geq \min(v_p(a), v_p(b))$. What can you say about $v_p(a + b)$ if $v_p(a) \neq v_p(b)$?