Honors Algebra II, Courant Institute, Spring 2022
http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2022/HonorsAlgebraII.html
Check the class forum for corrections and hints

Assignment 2

Due Thursday, Feb. 10.

These exercises build on each other. Each one uses results of previous exercises. Please do them in order. There are no textbook problems this week because this is enough, and because you will get plenty of practice with the textbook material when we get to real applications of it.

1. (*This exercise uses Greek letters for integers partly to practice using Greek letters. The material is part of elementary number theory, but presented here in the spirit of ring theory.*). The *greatest common divisor* of integers ξ and η is the positive integer $\gamma = \gcd(\xi, \eta)$ that generates the ideal generated by ξ and η:

$$\gamma = \gcd(\xi, \eta) \text{ means that } (\gamma) = (\xi, \eta) \;,\;\; \gamma \geq 1 \;.$$

This sequence of steps shows that the slick gcd definition is equivalent to the definition using common prime factors in ξ and η.

(a) Suppose p is a prime divisor of ξ and η. This is written $p|\xi$ and $p|\eta$. It means that there are (integers) α and β with $\xi = \alpha p$ and $\eta = \beta p$. Show that $p|\zeta$ for all $\zeta \in (\xi, \eta)$. Conclude that $p|\gamma$.

(b) Suppose that $\gamma = \gcd(\xi, \eta) > 1$. Show that there is a prime p with $p|\xi$ and $p|\eta$. *Hint.* $\xi \in (\gamma)$ and $p|\gamma$ for some p.

(c) Show that if $p|\xi$ and $p|\eta$, then $\gamma/p = \gcd(\xi/p, \eta/p)$.

(d) Suppose the ξ and η have prime factorizations

$$\xi = \prod p_i^{\mu_i} \;,\;\; \eta = \prod p_i^{\nu_i} \;.$$

This means that ξ has μ_1 copies of p_1 in its prime factorization, etc. Each product has finitely many terms, which means that there are finitely many i with $\mu_i > 0$ or $\nu_i > 0$. Show that $\gamma = \gcd(\xi, \eta)$ has prime factorization

$$\gamma = \prod p_i^{\lambda_i} \;,\;\; \lambda_i = \min(\mu_i, \nu_i) \;.$$

Hint. Use part (c) to "pull out prime factors" one at a time. Please take your time with this part. Try to find an argument that is "efficient", which means that it is clear and short. Some efficient arguments are clever, compared to "direct" arguments you might think of at first.

2. Let R be a ring and $a_k \in R$. Show that $(a_1, \cdots, a_n) = R$ if and only if there are $x_k \in R$ with $1 = x_1 a_1 + \cdots + x_n a_n$. Specialize this to $R = \mathbb{Z}$ as follows. Integers ξ and η are *relatively prime* if $\gcd(\xi, \eta) = 1$. Show that if ξ and η are relatively prime and n is any integer, then there are integers α and β with $n = \alpha\xi + \beta\eta$. This is a version of the *Chinese remainder theorem*, but give a proof using this Exercise and Exercise 1. *Comment.* Versions of this observation are used often.

3. This exercise defines the *Euler ϕ function*. It is interesting for itself (this exercise) and for the role it plays in the structure of integer multiplication mod n (next exercise). It is defined for $n \in \mathbb{Z}$, $n \geq 1$ (positive integers). It is the number of residues mod n that are relatively prime to n. More precisely, define the set of relatively prime residues as

$$G_n = \{k \text{ with } 1 \leq k \leq n-1 \text{ and } \gcd(k,n) = 1\} \ .$$

Then $\phi(n) = |G_n| =$ the number of residues in G_n.

   (a) Follow the definitions literally and show that $\phi(1) = 1$.

   (b) Let $q = p^r$ be a prime power. Identify G_q and find a formula for $\phi(p^r)$.

   (c) Let d be a positive divisor of n, so that n/d is a positive integer. Show that there is a 1-1 correspondence between the set of $m \in \{1, \cdots, n-1\}$ with $\gcd(m,n) = d$ and elements of $G_{n/d}$. *Hint.* First see how this works for $n = 10$ and its divisors $1, 2, 5$.

   (d) Prove Euler's ϕ formula (the sum is over all divisors of n)

$$n = \sum_{d|n} \phi(d) \ .$$

   Hint. Work out $n = 10$ or $n = 20$ or $n = 12$ to see how it happens.

4. Consider the operation of multiplication on residue classes of $k \in G_n$ mod n. Show that these form an abelian group. It's clearly associative and abelian, because it's multiplication mod n. The point is to find a multiplicative inverse. To find the multiplicative inverse of $x \in G_n$ (mod n), use the fact that $(x, n) = 1$.

5. There are two abelian groups of order 4, which are the cyclic group C_4 (addition mod 4) and the *Klein group* (terminology from the text), which is $C_2 \times C_2$. More precisely, any abelian group of order 4 is isomorphic either to C_4 of the Klein group. These groups are not isomorphic to each other (no element of the Klein group has order 4). Which one of these is the group G_8 is isomorphic to? *Comment.* This shows that G_n need not be a cyclic group. Exercise 7 shows that G_p is cyclic. Note that $|G_8| = |G_5| = 4$ (see Exercise 6 if you're not sure). The two groups have the same order (number of elements) but they're not isomorphic.

6. Define $\mathbb{F}_p = \mathbb{Z}/(p)$. This quotient is a ring. Show that it is a field by showing that G_p consists of the non-zero elements of $\mathbb{F}_p$ so each $x \in \mathbb{F}_p$ with $x \neq 0 \pmod{p}$ has a multiplicative inverse.

7. This sequence of steps shows that $\mathbb{F}_p^* \cong C_{p-1}$ (the cyclic group with $p-1$ elements). For each $x \in \mathbb{F}_p$, define the *order* to be

$$\text{ord}(x) = \min\left\{ \, k \text{ with } x^k = 1 \right\} \; .$$

The (multiplicative) *orbit* of x is the set of powers

$$\mathcal{O}(x) = \left\{ \, x^j \; , \; j \in \mathbb{Z} \, \right\} \; .$$

   (a) Show that $\text{ord}(x) = |\mathcal{O}(x)|$.

   (b) Show that if $\text{ord}(x) = k$, then $\mathcal{O}(x)$ is the set of all $y \in \mathbb{F}_p$ that satisfy the equation $y^k = 1$. *Comment.* This uses the fact that p is prime. We saw that G_8 has three elements of order 2.

   (c) Show that if $y \in \mathcal{O}(x)$ then $\text{ord}(y)|\text{ord}(x)$. Show that $\phi(k)$ is the number of elements of $\mathcal{O}(x)$ with order k. Show that $\phi(k)$ is the number of elements of $\mathbb{F}_p^*$ of order k. Show that $\text{ord}(x)|(p-1)$ (you can use a fact about the orders of subgroups of a finite group).

   (d) Show that there is at least one $x \in \mathbb{F}_p$ with $\text{ord}(x) = p-1$. *Hint.* Use Euler's ϕ formula (part (d) of Exercise 3) to get a contradiction. Be careful, part (c) does not, by itself, show there are elements of order d when $d|(p-1)$. You have to show this.

   (e) Show that the multiplicative group $\mathcal{O}(x)$ is isomorphic to C_k, where $k = \text{ord}(x)$. Conclude that $\mathbb{F}_p^* \cong C_{p-1}$.

   (f) Use part (e) to prove the little Fermat theorem, $x^{p-1} = 1 \pmod{p}$ for all $x \neq 0$.

8. An element $g \in \mathbb{F}_p$ with $\mathcal{O}(g) = \mathbb{F}_p^*$ is a *generator*, mod p. Show that 2 is a generator mod 5 but not mod 7. Find a generator mod 7. Every prime p has many generators, but they're not easy to identify except by direct calculation. It's natural to calculate $\mathcal{O}(2)$ as a first guess. If $2^{(p-1)/2} = -1$ (mod p), then 2 is a generator, otherwise not. The proof in Exercise 7 is *non-constructive*. It proves generators exist without telling you how to find them.

9. Let p be an odd prime. Show that the equation $x^2 = -1 \pmod{p}$ has a solution if and only if $p = 1 \pmod{4}$. *Hint.* $x = g^k$ for some k. Check (but don't hand in) that $2^2 = -1$ mod 5, there is no solution mod 7 (try all 4 possibilities). Find a solution mod 13 (to hand in).

10. The *Legendre symbol* is $\left(\dfrac{x}{p}\right)$. It records whether x is a square mod p:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x = y^2 \pmod{p} \text{ for some } y \in \mathbb{Z}, \; x \neq 0 \pmod{p} \\ 0 & \text{if } x = 0 \text{ (mod } p) \\ -1 & \text{otherwise .} \end{cases}$$

Show that the Legendre symbol is a (multiplicative) *character*, which means that, for any integers x and y and prime p,

$$\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right) .$$

Before doing the proof, but not to hand in, check that it's true for $p = 7$ and maybe $p = 11$. *Hint.* The only case that is deep (relies on real theorems) is when $\left(\frac{x}{p}\right) = -1$ and $\left(\frac{y}{p}\right) = -1$. Do the other cases first: x and y both squares, one of x or y equal to 0 mod p, $x = u^2$ $xy = v^2$, $x \neq 0$ and $y \neq 0 \pmod{p}$ implies y is a square. For the hard case, what can you say about k if g is a generator and $x = g^k$ and x is not a square?