Problem Set 1: Euclid and the Architecture of the Integers Student Handout

Divisibility, gcds, primes, and unique factorization

80 points + 10 optional challenge points

Name: _____ **Due:** _____

Purpose. This assignment develops the two complementary habits of elementary number theory: compute examples efficiently, then explain why the method works. Show the divisions in every use of Euclid's algorithm and name the theorem used in every proof.
You may use: the division algorithm, the Euclidean algorithm, Bézout's identity, Euclid's lemma, and the fundamental theorem of arithmetic. Unless a problem explicitly asks for a decimal answer, exact arithmetic is expected.

I. Divisibility and Euclid's algorithm

1. The invariant behind the algorithm. [6 points] Let $a, b, d, m, n \in \mathbb{Z}$.

(a) Prove that if $d \mid a$ and $d \mid b$, then $d \mid (ma + nb)$.

(b) Suppose $a = qb + r$. Prove that (a, b) and (b, r) have exactly the same common divisors. Conclude that $\gcd(a, b) = \gcd(b, r)$.

2. Three runs of Euclid's algorithm. [9 points] Compute each gcd, displaying every division. For part (c), describe the pattern in the remainders.

(a) $\gcd(2024, 748)$

(b) $\gcd(12345, 6789)$

(c) $\gcd(4181, 2584)$

3. Running Euclid backward. [12 points]

(a) Use the divisions from Problem 2(a) to express 44 as $2024x + 748y$ with $x, y \in \mathbb{Z}$.

(b) Find one integer solution of $2024x + 748y = 132$, and then find all integer solutions.

(c) Explain why $2024x + 748y = 100$ has no integer solution.

4. Useful gcd identities. [8 points]

(a) Prove that $\gcd(a + kb, b) = \gcd(a, b)$ for every $k \in \mathbb{Z}$.

(b) Use part (a), without factoring, to prove that $\gcd(2n + 1, n) = 1$ for every positive integer n.

(c) Prove that two consecutive positive integers are relatively prime.

5. Why the algorithm stops and succeeds. [7 points] In a paragraph, prove the Euclidean algorithm: explain both why repeated division must terminate and why the last nonzero remainder is the gcd of the original two positive integers.

II. Primes and unique factorization

6. Prime-exponent coordinates. [12 points]

(a) Find the prime factorizations of 7560 and 8820.

(b) Use the exponent vectors, without applying Euclid's algorithm, to find their gcd and lcm.

(c) How many positive divisors does 7560 have? Justify the counting rule you use.

(d) Verify numerically that $\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$ for this pair.

7. Euclid's lemma, the hinge of uniqueness. [8 points]

(a) Let p be prime. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$. You may use Bézout's identity.

(b) Deduce that if $p \mid a^m$ for an integer $m \geq 1$, then $p \mid a$.

(c) In two or three sentences, explain where part (a) enters the uniqueness proof in the fundamental theorem of arithmetic.

8. Two consequences of prime factorization. [8 points]

(a) Suppose $\gcd(a,b) = 1$ and ab is a perfect square. Prove that both a and b are perfect squares.

(b) Prove that $\sqrt{p}$ is irrational for every prime p.

9. There is no last prime. [10 points]

(a) Give Euclid's proof that there are infinitely many primes. Your proof must explicitly explain why the constructed integer has a prime divisor and why that divisor is new.

(b) The first six primes are $2, 3, 5, 7, 11, 13$. Compute their product plus one and verify

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

What common misunderstanding of Euclid's proof does this example correct?

Optional challenge

10. Infinitely many primes leaving remainder 3 upon division by 4. [10 extra points] Suppose, for contradiction, that the complete list of such primes is $p_1, \ldots, p_k$, and consider

$$N = 4p_1p_2 \cdots p_k - 1.$$

Prove that some prime divisor of N leaves remainder 3 upon division by 4, and that this divisor is not one of the p_i. Conclude that there are infinitely many primes of the form $4n + 3$.

The arithmetic is the evidence; the proof is the explanation.