Problem Set 2

Student handout

Euclid, continued fractions, and prime factorization

Week 2 | 100 points + 10 optional challenge points

Name: _____ **Due:** _____

Instructions. Show your divisions and use exact fractions. Justify every proof or counterexample. You may use the division algorithm, Bézout's identity, and Euclid's lemma. You may use the fundamental theorem of arithmetic except when proving it in Problem 4.

Notation. A finite simple continued fraction is

$$[a_0; a_1, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}, \qquad [a_0] = a_0.$$

Here a_0 is an integer and a_i is a positive integer for $i \geq 1$. Unless otherwise requested, use $a_n \geq 2$ when $n \geq 1$.

I. Euclid and continued fractions

1. One calculation, two readings

[14 points]

(a) Use the Euclidean algorithm to compute $\gcd(301, 133)$. (5)

(b) Work backward to find integers x, y such that $301x + 133y = \gcd(301, 133)$. Check your answer by substitution. (4)

(c) Use the quotients from (a) to express $301/133$ as a simple continued fraction. Reduce $301/133$ to lowest terms and explain why this does not change its continued-fraction expansion. (5)

2. Unfolding a continued fraction

[12 points]

(a) Evaluate $[2; 3, 4]$ and $[0; 2, 1, 3]$ as fractions in lowest terms. (4)

(b) For $n \geq 1$ and $a_n \geq 2$, prove the identity

$$[a_0; a_1, \dots, a_n] = [a_0; a_1, \dots, a_{n-1}, a_n - 1, 1].$$

Explain the equality by looking at the end of the nested fraction. (4)

(c) Give a second expansion, ending in 1, for each number in (a). (4)

3. Bounding a square root with fractions

[12 points]

Consider the four truncations

$$c_0 = [1], \qquad c_1 = [1; 2], \qquad c_2 = [1; 2, 2], \qquad c_3 = [1; 2, 2, 2].$$

Such truncations are called *convergents*.

(a) Compute the four fractions in lowest terms. (4)

(b) Decide which are below $\sqrt{2}$ and which are above it by comparing their squares with 2. Do not use decimal approximations. (4)

(c) Using these values, give the narrowest interval you can with a lower endpoint below $\sqrt{2}$ and an upper endpoint above it. Find its exact width. (4)

II. Unique factorization and its consequences

4. Why factorization exists and is unique [14 points]

Prove the fundamental theorem of arithmetic in the following steps.

(a) Use strong induction to prove that every integer $n > 1$ is a product of primes. Treat the prime and composite cases separately. (6)

(b) Suppose $p_1 \cdots p_r = q_1 \cdots q_s$, where all factors are prime. Use Euclid's lemma to match and cancel prime factors. Explain why this process proves uniqueness up to order, including why one side cannot have factors left over. (6)

(c) Why would allowing 1 as a prime destroy this uniqueness statement? (2)

5. Completing a square or a cube [14 points]

Let $N = 5400$.

(a) Find the prime factorization of N. (4)

(b) Find the least positive integer k for which Nk is a perfect square. Give the square root of Nk and prove that your k is least. (5)

(c) Find the least positive integer ℓ for which $N\ell$ is a perfect cube. Give the cube root of $N\ell$ and prove minimality. (5)

6. True, false, or missing a hypothesis? [12 points]

All variables below are positive integers.

(a) Prove or disprove: if $a^2 \mid b^2$, then $a \mid b$. (3)

(b) Prove or disprove: if $a \mid b^2$, then $a \mid b$. (3)

(c) Give a counterexample to the claim that $a \mid c$ and $b \mid c$ imply $ab \mid c$. Then prove that the claim becomes true when $\gcd(a, b) = 1$. (6)

III. Finding primes and knowing when to stop

7. The sieve of Eratosthenes [12 points]

(a) Use the grid to sieve the integers from 2 through 120. Mark 1 as neither prime nor composite. Process primes in increasing order, crossing out their multiples beginning at their squares. List all primes that remain and give their total number. (8)

(b) The numbers 91 and 119 survive the passes for $2, 3, 5$. Explain why they are nevertheless composite and identify the pass that removes them. (4)

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

8. Why the sieve works [10 points]

(a) Prove that every composite integer $n > 1$ has a prime divisor at most $\sqrt{n}$. Deduce that sieving by all primes $p \le \sqrt{N}$ removes every composite integer at most N. (4)

(b) Explain why the pass for a prime p may begin at p^2: every multiple mp with $2 \le m < p$ has already been removed. Your argument must also cover composite m. (4)

(c) Would the sieve always work if we used only primes $p < \sqrt{N}$? Give a counterexample showing why the equality matters. (2)

Optional challenge: a square equals a cube [10 extra points]

Let a, b be positive integers satisfying $a^2 = b^3$. Prove that there is a positive integer t such that $a = t^3$ and $b = t^2$. *Hint:* compare the exponents of a fixed prime on the two sides.