Number Theory Midterm I

RDB

June 14, 2023

I feel fine today modulo a slight headache.
— *The Hacker's Dictionary*

INSTRUCTIONS No outside materials (notes, textbook, internet) or resources (calculators). Write your name on the big line below.

Good luck,

Name: ____!

Problem 1 Find the general solution to

$$42x + 35y = 2,$$

or prove that no solutions exist. (10 points)

Solution 1
The gcd of 42 and 35 is 7, which does not divide 2, so there are no solutions.

Problem 2 Fix integers a and b. Suppose that $ax + by = p$ for some integers x and y and a prime p. Prove that $\gcd(a, b)$ is either 1 or p. (10 points)

Solution 2
By a theorem in class (or writing $a = \gcd(a, b)k$ and $b = \gcd(a, b)j$), we see that $\gcd(a, b)$ divides p, so it is either 1 or p since p is prime.

Problem 3

(**a**) Use the Euclidean algorithm to compute the greatest common divisor of 153 and 64. (5 points)

(**b**) By reversing the Euclidean algorithm, find integers x and y such that $153x + 64y = \gcd(153, 64)$. (5 points)

Solution 3
I don't want to type this up. I showed how to do it in class. Come bother me if you want to see it again!

Problem 4 List three integer solutions (x, y) to

$$38x + 15y = 1,$$

if any exist. (10 points)

Solution 4
The gcd of 38 and 15 is 1, so solutions *do* exist. The Euclidean algorithm will give $x_0 = 2$ and $y_0 = -5$, so the general solution is

$$x = 2 + 15t; \qquad y = -5 - 38t$$

for an integer t. Shifting up and down once gives the solutions $(2, -5)$, $(17, -43)$, $(-13, 33)$.

Problem 5 Write $(1024)_5$ in base 10. (5 points)

Solution 5

$$\begin{aligned}(1024)_5 &= 1 \cdot 5^3 + 0 \cdot 5^2 + 2 \cdot 5^1 + 4 \cdot 5^0 \\ &= 125 + 10 + 4 \\ &= 139.\end{aligned}$$

Problem 6 Write 76 in base 3. (5 points)

Solution 6
The largest power to begin with is $3^3 = 27$, and we can fit 2 of them in:

$$76 - 2 \cdot 3^3 = 22.$$

Repeating:

$$22 - 2 \cdot 3^2 = 4$$

Again:

$$4 - 1 \cdot 3 = 1$$

Finally:

$$1 = 1 \cdot 3^0.$$

So

$$\begin{aligned} 76 &= 2 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3^1 + 1 \cdot 3^0 \\ &= (2211)_3. \end{aligned}$$

Problem 7 Translate the following numbers from binary into base 10:

(a) $(1)_2$ (1 point)

(b) $(11)_2$ (1 point)

(c) $(101)_2$ (1 point)

(d) $(11010)_2$ (1 point)

(e) $(100110)_2$ (1 point)

Solution 7
I don't want to type this one up either. Come see me if you want a demonstration!

Problem 8

(a) State Fermat's theorem. (5 points)

(b) Prove that $2^n \equiv 1 \pmod 3$ if n is even, and $2^n \equiv 2 \pmod 3$ if n is odd. (10 points)

Solution 8

(a) If p is prime and does not divide a, then $a^{p-1} \equiv 1 \pmod p$.

(b) By Fermat, $2^{3-1} = 4 \equiv 1 \pmod 3$. If n is even, say $n = 2k$, then $2^n = 4^k \equiv 1^k = 1 \pmod 3$. If n is odd, say $n = 2k + 1$, then $2^n = 4^k \cdot 2 \equiv 2 \pmod 3$.

Problem 9

(a) Prove that $\gcd(a, b) = \gcd(a - b, b)$ for any integers a and b. (10 points)

(b) Prove that $\gcd(F_n, F_{n+1}) = 1$ for $n \geq 1$, where F_n is the nth Fibonacci number, defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 1$. (10 points)

Solution 9

(a) If d divides a and b, then it also divides $a - b$, so the common divisors of (a, b) are common divisors of $(a - b, b)$. Conversely, if d divides $a - b$ and b, then it also divides $(a - b) + b = a$, so the common divisors of $(a - b, b)$ are common divisors of (a, b). Together, this means that the set of common divisors of (a, b) equals the set of common divisors of $(a - b, b)$; in particular, $\gcd(a, b) = \gcd(a - b, b)$.

(b) Note that $\gcd(F_n, F_{n+1}) = \gcd(F_n, F_{n+1} - F_n) = \gcd(F_n, F_{n-1})$ for all $n \geq 1$. It follows (by induction) that $\gcd(F_n, F_{n+1})$ is constant for all $n \geq 1$, so $\gcd(F_n, F_{n+1}) = \gcd(F_1, F_2) = 1$ for all $n \geq 1$.

Problem 10 I have decided that you, dear student, deserve 100 points on this exam. You were excellent for 7 questions, and mediocre for 3 questions. I want to assign a weight x to your excellent questions, and a weight y to your not so excellent questions, so that you get a total of

$$7x + 3y = 100$$

points. Is is possible to do this with positive, integer weights? How many ways can I do it? (10 points)

Solution 10
A particular solution to this Diophantine equation is $x = y = 10$, so every solution is $(10, 10)$ shifted by multiples of $(\pm 3, \mp 7)$. Positive solutions from shifting x down:

$$(7, 20),\ (4, 30),\ (1, 40).$$

Positive solutions from shifting y up:

$$(13, 3).$$

And we started with $(10, 10)$, so there are five total ways to do it.

BONUS PROBLEM The exam is graded out of 100 points, all accounted for in the previous problems. The following problem is worth an additional 10 points.

Problem 11 Write the prime factorization of n as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},$$

where the p_k are distinct primes and the e_k's are positive integers. Prove that n has

$$(e_1 + 1)(e_2 + 1) \cdots (e_m + 1)$$

distinct positive divisors.

Solution 11
For each $i = 1, 2, \ldots, m$, every divisor of n has some number of factors of p_i, from none to e_i of them. There are therefore $e_i + 1$ ways to choose the p_i factor, which means there are $(e_1+1)(e_2+1) \cdots (e_m+1)$ ways to choose the prime factors all together. The resulting divisors are distinct because their prime factorizations are distinct.