Solutions

Department of Mathematics

University of Pittsburgh

MATH 1020 (Number theory)

Midterm 1, Fall 2018

Instructor: Kiumars Kaveh

Last Name: **Student Number:**

First Name:

TIME ALLOWED: 1 HOUR AND 20 MINUTES. TOTAL POINTS: 100
NO AIDS ALLOWED. WRITE SOLUTIONS ON THE SPACE PROVIDED.
PLEASE READ THROUGH THE ENTIRE TEST BEFORE STARTING AND TAKE NOTE OF HOW MANY POINTS EACH QUESTION IS WORTH.
FOR FULL MARK YOU MUST PRESENT YOUR SOLUTION CLEARLY.

Question	Mark
1	/15
2	/10
3	/10
4	/20
5	/20
6	/10
7	/15
8	2
TOTAL	/100

1(a).[10 points] State the following theorems: Dirichlet's theorem (on prime numbers in an arithmetic progression), and the prime number theorem (on distribution of primes).

Dirichlet's thm: Let $(a,b)=1$, $a,b \in \mathbb{N}$. Then the set $\{ak+b \mid k \in \mathbb{N}\}$ contains infinitely many primes.

Prime number theorem: Let $\pi(x) = \left| \left\{ p \;\middle|\; \begin{array}{l} 1 \leq p < x \\ p \text{ prime} \end{array} \right\} \right|$

Then $\pi(x) \sim \dfrac{x}{\ln x}$, that is: $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x/\ln x} = 1$.

1(b).[5 points] Define the greatest common divisor of two numbers.

$d = (a,b)$ if:

① $d \mid a$ & $d \mid b$

② If $c \mid a$ & $c \mid b$ then $c \mid d$.

2.[10 points] Let a and b be positive integers. Prove that the greatest common divisor $d = (a, b)$ is the smallest positive integer that can be written as a linear combination $ax + by$ for some $x, y \in \mathbb{Z}$.

Let $S = \left\{ ax+by \;\middle|\; \begin{array}{l} x, y \in \mathbb{Z} \\ ax+by > 0 \end{array} \right\}$ and $d' = \min S$, $d' = ax_0 + by_0$

Let $a = qd' + r \Rightarrow r = a - qd' = a - qax_0 - qby_0 = a(1-qx_0) + b(-qy_0)$

which shows that $r \in S$ or $r = 0$. If $r \in S$ then $r < d'$ which is not possible so $r = 0$ i.e. $d' | a$. Similarly $d' | b$

& thus d' is a common divisor of a & b.

Now if $c | a$ & $c | b$ then $c | ax_0 + by_0 = d'$.

This proves that d' is the greatest common divisor of a & b.

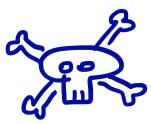
3(a).[5 points] Let $n > 1$ be an integer and let p be the smallest prime factor of n. Show that if $p > n^{1/3}$ then either n/p is a prime or is equal to 1.

Suppose n/p is neither 1 nor a prime. Then it has at least two prime factors q_1, q_2. That is, $\frac{n}{p} = q_1 q_2 x$ for some $x \geq 1$.

By ass. p is the smallest prime factor in n, hence $p \leq q_1, q_2$

$\Rightarrow \frac{n}{p} = q_1 q_2 x \geqslant p^2 x \geqslant p^2 \Rightarrow n \geqslant p^3 \Rightarrow n^{1/3} \geqslant p$ which

Contradicts $p > n^{1/3}$



3(b).[5 points] Prove that $\sqrt[3]{2+\sqrt{7}}$ is an irrational number.

Let $\alpha = \sqrt[3]{2+\sqrt{7}}$ then $\alpha^3 = 2+\sqrt{7} \Rightarrow (\alpha^3-2)^2 = 7$

$\Rightarrow (\alpha^3-2)^2 - 7 = 0$ i.e. α is a root of the monic poly. (with int. coeff.) $x^6 - 4x^3 + \underset{-3}{\cancel{4-7}}$.

By a thm. from class α is either irr. or an integer.

But $1 < \sqrt[3]{2+\sqrt{7}} < 2$ because $4 < 7 < 9 \Rightarrow 2 < \sqrt{7} < 3 \Rightarrow$

$4 < 2+\sqrt{7} < 5 \Rightarrow 1 < \sqrt[3]{4} < \sqrt[3]{2+\sqrt{7}} < \sqrt[3]{5} < \sqrt[3]{8} = 2$.

So $\sqrt[3]{2+\sqrt{7}}$ not an integer.

Alt. solution: $\sqrt{7}$ is irr. because suppose $\sqrt{7} = \frac{p}{q}$ with $(p,q) = 1$.

Then $7q^2 = p^2 \Rightarrow 7 \mid p^2 \Rightarrow 7 \mid p \Rightarrow 7^2 \mid 7q^2 \Rightarrow 7 \mid q^2 \Rightarrow 7 \mid q$, contradicts $(p,q)=1$.

Now if $\sqrt[3]{2+\sqrt{7}} = \frac{a}{b}$ where $a,b \in \mathbb{Z}$ then $2+\sqrt{7} = \frac{a^3}{b^3} \Rightarrow \sqrt{7} = \frac{a^3}{b^3} - 2$ is rational, Contradiction to above.

4(a).[10 points] Find the (multiplicative) inverse of 97 (*mod* 121).

$121 x_0 + 97 y_0 = 1$

$121 = 97 \cdot 1 + 24$

$97 x_1 + 24 y_1 = 1 \rightsquigarrow x_1 = x_0 + y_0$, $y_1 = x_0$

$97 = 24 \cdot 4 + 1$

$24 x_2 + 1 \cdot y_2 = 1 \rightsquigarrow x_2 = y_1 + 4x_1$, $y_2 = x_1$

$x_2 = 1$, $y_2 = -23 \Rightarrow y_1 = 1 - 4(-23) = 93$, $x_1 = -23 \Rightarrow y_0 = (-23) - 93 = -116$

$-116 \equiv 5 \pmod{121}$

$$\boxed{97^{-1} \equiv 5 \pmod{121}}$$

4(b).[10 points] Write the number $(1201)_{10}$ in base 8.

$1201 = 8 \cdot 150 + 1 \longrightarrow a_0 = 1$

$150 = 8 \cdot 18 + 6 \longrightarrow a_1 = 6$

$18 = 8 \cdot 2 + 2 \longrightarrow a_2 = 2$

$2 = 0 \cdot 2 + 2 \longrightarrow a_3 = 2$

$$\boxed{(1201)_{10} = (2261)_8}$$

5(a).[10 points] Solve the linear congruence $25x \equiv 10$ $(mod\ 160)$. How many incongruent solutions (mod 160) does it have? $160/5 = 32$

$25x \equiv 10 \pmod{160} \iff 5x \equiv 2 \pmod{32}$

$5^{-1} \bmod 32 = 13 \qquad (13 \times 5 = 65 \equiv 1 \pmod{32})$

$x \equiv (5^{-1}) \cdot 2 \equiv 26 \pmod{32}$

There are 5 incongruent sol. mod 160.

$5 = \gcd(25, 160)$

$\boxed{26 + 32k \qquad k = 0, 1, 2, 3, 4}$

5(b).[10 points] Find smallest positive solution of the system of congruences:

$$x \equiv 1\ (mod\ 3)$$
$$x \equiv 2\ (mod\ 5)$$
$$x \equiv 3\ (mod\ 7)$$

$x = \underbrace{M_1}_{5\cdot 7}\underbrace{y_1}_{2 = (35)^{-1} \bmod 3}\underbrace{a_1}_{1} + \underbrace{M_2}_{21}\underbrace{y_2}_{1 = 21^{-1} \bmod 5}\underbrace{a_2}_{2} + \underbrace{M_3}_{15}\underbrace{y_3}_{1 = 15^{-1} \bmod 7}\underbrace{a_3}_{3}$

$x = 35 \cdot 2 \cdot 1 + 21 \cdot 2 \cdot 1 + 15 \cdot 1 \cdot 3 = 157 \equiv 52 \pmod{105}$

$105 = 3 \times 5 \times 7$

$\boxed{\text{52 smallest positive solution of the system.}}$

6.[10 points] Recall that the Fibonacci numbers f_n are defined inductively as follows: $f_1 = 1$, $f_2 = 1$ and for $n > 2$, $f_n = f_{n-1} + f_{n-2}$. Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Prove that for all $n \geq 1$ we have:

$$f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Hint: α, β are roots of $x^2 - x - 1 = 0$.

$$f_1 = \frac{\alpha - \beta}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 \qquad f_2 = \frac{\alpha^2 - \beta^2}{\sqrt{5}} = \frac{\alpha - \beta}{\sqrt{5}} \cdot \alpha + \beta = \alpha + \beta = 1.$$

$$f_{n-1} + f_n = \frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{5}} + \frac{\alpha^n + \beta^n}{\sqrt{5}} = \frac{(\alpha^{n-1} + \alpha^n) - (\beta^{n-1} + \beta^n)}{\sqrt{5}}$$

$$= \frac{\alpha^{n-1}(1+\alpha) - (\beta^{n-1}(1+\beta))}{\sqrt{5}} \quad \text{but} \quad \begin{matrix} 1+\alpha = \alpha^2 \\ 1+\beta = \beta^2 \end{matrix} \quad \text{so}$$

$$= \frac{\alpha^{n-1} \cdot \alpha^2 - \beta^{n-1} \cdot \beta^2}{\sqrt{5}} = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} = f_{n+1}.$$

7.[15 points] Find all solutions of the polynomial congruence:

$$x^3 + 8x + 4 \equiv 0\ (mod\ 250).$$

Hint: $250 = 2 \cdot 5^3$, use Hensel's lemma.

$250 = 2 \times 125 = 2 \times 5^3$

Need to find sol. for $\begin{cases} x^3 + 8x + 4 \equiv 0 \pmod 2 & (1) \\ x^3 + 8x + 4 \equiv 0 \pmod{5^3} & (2) \end{cases}$

(1) $x^3 + 8x + 4 \equiv x^3 \equiv 0 \pmod 2 \Rightarrow x \equiv 0 \pmod 2$

(2) First we solve $x^3 + 8x + 4 \equiv 0 \pmod 5 \Rightarrow x \equiv -1, -2 \pmod 5$

- $f'(x) = 3x^2 + 8$ $\quad \underline{x \equiv -1 \pmod 5}$ $\quad f'(-1) = 3 + 8 \equiv 1 \pmod 5$ $\not\equiv 0$

By Hensel's Lemma: $r_1 = -1 \Rightarrow \boxed{r_2 = r_1 - \left(f(r_1) \cdot f'(r_1)^{-1}\right)}$

$= (-1) - (-5) \cdot 1$

$= 4$

check:

$\left(f(4) = 4^3 + 8 \cdot 4 + 4 = 100 \equiv 0 \pmod{5^2} \right)$

Again: $r_3 = r_2 - f(r_2) \cdot f'(r_1)^{-1} = 4 - 100 \cdot 1 = -96$

Since $-96 \equiv 0 \pmod 2$, $\underline{x = -96 \text{ is a sol. for } x^3 + 8x + 4 \equiv 0 \pmod{250}}$

- $\underline{x \equiv -2 \pmod 5} \Rightarrow f'(-2) = 3 \cdot 4 + 8 \equiv 0 \pmod 5$

$f(-2) = -8 - 16 + 4 = -20 \not\equiv 0 \pmod{5^2}$ so (by second part of Hensel's Lemma)

no solution mod 5^2 & hence mod 5^3.

8.[2 points] Draw the cartoon face of a number theorist.