Solutions

Name:

M403 - Fall 2012 - Dr. A. Lindenstrauss

MIDTERM 2

10 pts

① Let $a, b \in \mathbb{Z}$ and let $d = \gcd(a, b)$. Assume $d > 0$. Prove (without using prime factorization — directly from definitions) that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

The gcd of any two integers which are not both zero is at least 1, and we know $d>0$ so $(a,b) \neq (0,0)$, hence $(\frac{a}{d}, \frac{b}{d}) \neq (0,0)$. Assume by contradiction that $\gcd(\frac{a}{d}, \frac{b}{d}) = c > 1$. Then there exist $x, y \in \mathbb{Z}$ with $\frac{a}{d} = cx$, $\frac{b}{d} = cy$. So $a = cdx$, $b = cdy$ and cd is a common divisor of a & b. But recall our assumptions that $d > 0$, $c > 1$. This implies $cd > d$, in contradiction to d being the greatest common divisor. So having $c > 1$ was impossible, and $c = 1$.

10 pts

② Prove that $\sqrt{7}$ is irrational. Write carefully, explaining every step.

Proof by contradiction: Assume $\sqrt{7}$ were equal to a rational number $r \in \mathbb{Q}$. A lemma we proved showed that any rational number could be written in lowest terms, $r = \frac{a}{b}$ with $b \neq 0$ and $\gcd(a,b) = 1$. So write $\sqrt{7} = \frac{a}{b}$ with $b \neq 0$ and $\gcd(a,b) = 1$. WLOG we can assume $a, b > 0$ (otherwise replace them by $-a, -b$). Square both sides to get $7 = \frac{a^2}{b^2}$

$$\Rightarrow 7b^2 = a^2$$

Now 7 is prime and divides $7b^2 = a^2 = a \cdot a \Rightarrow 7$ divides a, and I can write $a = 7c$, $c \in \mathbb{Z}$. $7b^2 = a^2 = 49c^2 \Rightarrow b^2 = 7c^2$. By the same argument, 7 divides b. So then $\gcd(a,b) \geq 7$, $\gcd(a,b) \neq 1$. Contradiction. $\sqrt{7} \notin \mathbb{Q}$

10 pts

(3) Let p be a prime and let a be an integer for which $0 < a < p$.
Prove that $a^{p-1} \equiv 1 \pmod{p}$
Hint: $a^p - a = a(a^{p-1} - 1)$

By Fermat's Little theorem, since p is prime $a^p \equiv a \pmod{p}$.
that is: p divides $a^p - a = a(a^{p-1} - 1)$.
Since p is prime, that means that p divides either a (which it can't: for any $k \in \mathbb{Z}$, $|kp| = 0$ (if $k=0$) or $|kp| \geq p$ (if $k \neq 0$), so we never get $kp = a$ for $0 < a < p$) or $a^{p-1} - 1$. Since p cannot divide a, it must divide $a^{p-1} - 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.

10 pts

(4) Let $a, b \in \mathbb{Z}$ and let $d = \gcd(a, b)$.
a) Show that if $c = s \cdot a + t \cdot b$ for some $s, t \in \mathbb{Z}$ then d must divide c.
b) Does d have to be equal to c in a)? Prove that it does have to be equal, or give a counter-example

a) Clearly if d divides both a & b, there are $x, y \in \mathbb{Z}$ for which $a = dx$, $b = dy$. Then
$c = sa + tb = sdx + tdy = d(sx + ty) \Rightarrow d \mid c$.

b) No! e.g. I can take $s = t = 0$ & get $c = 0$ in situations where $d > 0$. Or I can take $s = 1000$, $t = 0$ & get $c = 1000a$ which if $a \neq 0$ is not a divisor of a. The gcd d is just one of infinitely many linear combinations (unless $a = b = 0$).

10 pts

5) a) Let m, m' be positive integers, let $b, b' \in \mathbb{Z}$, and let $d = \gcd(m, m')$. Show that if there exists a solution $x \in \mathbb{Z}$ to the system $\begin{cases} x \equiv b \pmod{m} \\ x \equiv b' \pmod{m'} \end{cases}$

then d divides $b - b'$. (Hint: write $b - b'$ in terms of m & m').

If there is such a solution x, then there exist $k, l \in \mathbb{Z}$ so that $\begin{cases} x = km + b \\ x = lm' + b' \end{cases}$ And so

$km + b = lm' + b'$, and $b - b' = (-k)m + lm'$ is a linear combination of m & m'. By 4) a), $b - b'$ must be divisible by $d = \gcd(m, m')$.

10 pts

b) Show that if d divides $b - b'$, you can solve the system $\begin{cases} x \equiv b \pmod{m} \\ x \equiv b' \pmod{m'} \end{cases}$

To solve the system, you first need to solve the first equation. All the solutions to it are of the form $x = km + b$, $k \in \mathbb{Z}$. So we need $x = km + b$ for which $km + b \equiv b' \pmod{m'}$

$$km \equiv b' - b \pmod{m'}$$

We showed that the equation $ax \equiv c \pmod{m'}$ has a solution $\Leftrightarrow$ $\gcd(a, m')$ divides c

In our case, we are trying to solve $km \equiv b' - b \pmod{m'}$ for k, and since we know $\gcd(m, m')$ divides $b' - b$ (which is equivalent to dividing $b - b'$), there is a solution.

5 pts

(6) a) Use the Euclidean algorithm to find $\gcd(652, 156)$

$652 = \overbrace{4 \cdot 156}^{624} + 28 \Rightarrow \gcd(652,156) = \gcd(156, 28)$

$156 = \overbrace{5 \cdot 28}^{140} + 16 \Rightarrow \gcd(156, 28) = \gcd(28, 16)$

$28 = 1 \cdot 16 + 12 \Rightarrow \gcd(28, 16) = \gcd(16, 12)$

$16 = 1 \cdot 12 + 4 \Rightarrow \gcd(16, 12) = \gcd(12, 4)$

$12 = 3 \cdot 4 \qquad \gcd(12, 4) = 4$

$\Rightarrow \gcd(652, 156) = 4$

5 pts

b) Use your work in a) to find a way of writing $\gcd(652, 156)$ as a linear combination (with integer coefficients) of 652 and 156

$4 = 16 - 12 = 16 - (28 - 16) = -28 + 2 \cdot 16 = -28 + 2(156 - 5 \cdot 28)$

$= 2 \cdot 156 - 11 \cdot 28 = 2 \cdot 156 - 11(652 - 4 \cdot 156) = -11 \cdot 652 + 46 \cdot 156$

$4 = -11 \cdot 652 + 46 \cdot 156$

5 pts

(7) a) Find $s, t \in \mathbb{Z}$ for which $s \cdot 4 + t \cdot 49 = 1$.

$s = -12 \qquad t = 1$

$-12 \cdot 4 + 1 \cdot 49 = 1$

5 pts

b) Use your work in a) to solve $4x \equiv 5 \pmod{49}$

a) tells me that for $y = -12$,

$4y \equiv 1 \pmod{49}$

$\Rightarrow 4 \cdot 5y \equiv 5 \cdot 1 \equiv 5 \pmod{49}$

so I need to take $x \equiv 5 \cdot -12 \equiv -60 \pmod{49}$

For example, I can take $x = 38$ ($38 \equiv -60 \pmod{49}$ because 49 divides 98). Check:

$4 \cdot 38 = 152 = 147 + 5 = 3 \cdot 49 + 5 \equiv 5 \pmod{49}$

5 pts

8) Find $\gcd(3^2 \cdot 5^3 \cdot 7^4 \cdot 11^5,\ 3^6 \cdot 5^5 \cdot 7^4 \cdot 13^2 \cdot 17)$
(no need to multiply it out)

$3^2 \cdot 5^3 \cdot 7^4$

5 pts

9) a) Give the general form of a solution to the system

$$\begin{cases} 2x \equiv 3 \pmod 5 \\ 3x \equiv 5 \pmod 7 \end{cases}$$

To solve the first, I need $x = 5k+4$ for some $k \in \mathbb{Z}$

$3(5k+4) \equiv 5 \pmod 7 \iff 15k + 12 \equiv 5 \pmod 7$

$\iff k + 5 \equiv 5 \pmod 7 \iff k \equiv 0 \pmod 7$

General sol'n: $x = 35\ell + 4 \quad \ell \in \mathbb{Z}$

5 pts

b) Give the general form of a solution to the system
$$\begin{cases} 2x \equiv 3 \pmod 5 \\ 3x \equiv 5 \pmod 7 \\ x \equiv 1 \pmod 2 \end{cases}$$

To solve the first two, I need $x = 35\ell + 4$ for some $\ell \in \mathbb{Z}$. This is odd $\iff \ell$ is odd, so

$x = 70m + 35 + 4 = 70m + 39$ for $m \in \mathbb{Z}$

5 pts

10) Can you solve the system
$$\begin{cases} 2x \equiv 5 \pmod{12} \\ x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod{11} \end{cases}$$
? Justify your answer.

No, for any $x \in \mathbb{Z}$, $2x$ is even so can never be of the form $5 + k \cdot 12$ for $k \in \mathbb{Z}$.
So the first equation has no solution, so the system cannot have a solution.