SOLUTIONS Name:

M403 – Fall 2011 – Dr. A. Lindenstrauss
MIDTERM 2

① 20 pts Let F_i be the i'th Fibonacci number, $F_0 = 0$, $F_1 = 1$, and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Show that for all $n \geq 0$, $\gcd(F_n, F_{n+1}) = 1$. (Hint: use induction on n).

Recall a homework problem in which you proved that $\gcd(a-b, b) = \gcd(a, b)$ (the point was that for an integer d which divides b, $d \mid a \Leftrightarrow d \mid a-b$)

Proof by induction on n that $\gcd(F_n, F_{n+1}) = 1$ for $n \geq 0$:

Base case: $n = 0$, $\gcd(F_0, F_1) = \gcd(0, 1) = 1$ because 1's divisors are ± 1, anything divides 0 so the greatest common divisor is 1.

Inductive step: Assume $\gcd(F_{n-1}, F_n) = 1$ and show that $\gcd(F_n, F_{n+1}) = 1$:

Recall that $F_{n+1} = F_n + F_{n-1}$.

$$\gcd(F_n, F_{n+1}) \underset{\substack{\uparrow \\ \gcd(a,b)=\gcd(b,a) \\ \text{for any } a, b}}{=} \gcd(F_{n+1}, F_n) = \gcd(F_n + F_{n-1}, F_n) =$$

$$\underset{\substack{\nearrow \\ \text{by HW} \\ \text{problem}}}{=} \gcd(F_n + F_{n-1} - F_n, F_n) = \gcd(F_{n-1}, F_n) \underset{\substack{\uparrow \\ \text{by inductive} \\ \text{hypothesis}}}{=} 1$$

18 pts

② Prove the Chinese Remainder Theorem: That if $m_1, m_2 > 0$ are integers and $\gcd(m_1, m_2) = 1$, then for any $a_1, a_2 \in \mathbb{Z}$ you can solve the system

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{cases}$$

with some $x \in \mathbb{Z}$. (You do not need to prove, though it is true, that any two solutions differ by a multiple of $m_1 \cdot m_2$).

To solve the first equation, we will need to have $x = k \cdot m_1 + a_1$ for some $k \in \mathbb{Z}$. For such an x to solve the second equation, we need to have

$$k \cdot m_1 + a_1 \equiv a_2 \mod m_2$$

$$k \cdot m_1 \equiv (a_2 - a_1) \mod m_2$$

Since $\gcd(m_1, m_2) = 1$, this can be solved: there exist $s, t \in \mathbb{Z}$ for which

$$s \cdot m_1 + t \cdot m_2 = 1$$

$$\Rightarrow \quad s \cdot m_1 \equiv 1 \mod m_2$$

$$\Rightarrow \quad s(a_2 - a_1) \cdot m_1 \equiv (a_2 - a_1) \mod m_2$$

Take $k = s(a_2 - a_1)$

$x = s(a_2 - a_1) m_1 + a_1$ solves both equations, and is in $\mathbb{Z}$ because $a_1, a_2, m_1,$ & s are all in $\mathbb{Z}$.

20 pts

3. Prove Fermat's little theorem for $a \geq 0$: that if p is a prime and $a \in \mathbb{N}$, $\underbrace{a^p}_{\text{a raised to the power } p} \equiv a \mod p$.

Induction on a: Base case: $a=0$, $0^p = 0$ so certainly $0^p \equiv 0 \mod p$.

Inductive step: Assume that $a>0$ & $(a-1)^p \equiv a-1 \mod p$.

Recall that $(b+c)^p = b^p + \sum_{i=1}^{p-1} \underbrace{\binom{p}{i}}_{\text{divisible by } p} b^{p-i} c^i + c^p$

for any $b, c \in \mathbb{Z}$ so $(b+c)^p \equiv b^p + c^p \mod p$ for any $b, c \in \mathbb{Z}$. Thus

$a^p = ((a-1)+1)^p \equiv (a-1)^p + 1^p \equiv a-1+1 \equiv a \mod p$

by inductive hypothesis, $(a-1)^p \equiv a-1 \mod p$
by direct calculation, $1^p = 1$

$a^p \equiv a \mod p$

20 pts

4. a) Let $f: X \to Y$ and $g: Y \to Z$ be functions. Assume that $g \circ f$ is injective, and show that f must be injective.

b) Let f and g be as in a). Assume that $g \circ f$ is injective and that f is surjective, and show that g must be injective.

a) Say $f(a) = f(b)$ for $a, b \in X$. Then
$g(f(a)) = g(f(b))$
$\Rightarrow (g \circ f)(a) = (g \circ f)(b) \underset{g \circ f \text{ is injective}}{\Rightarrow} a = b$. Thus f is injective.

b) Say $g(c) = g(d)$ for $c, d \in Y$. Since f is surjective, there exist $a, b \in X$ with $c = f(a)$, $d = f(b)$. So I have $g(f(a)) = g(f(b)) \Rightarrow (g \circ f)(a) = (g \circ f)(b) \underset{g \circ f \text{ is inj}}{\Rightarrow} a = b$
$\Rightarrow c = f(a) = f(b) = d$. Thus g is injective

⑤ Short answer - show your work but no justification needed.

3pts a) What are the possible remainders of perfect squares mod 3? 0 & 1

b/c $0^2 \equiv 0 \mod 3$, $1^2 \equiv 1 \mod 3$, & $2^2 \equiv 1 \mod 3$

(and $a \overset{\text{mod } 3}{\equiv} b \Rightarrow a^2 \equiv b^2 \mod 3$)

3pts b) What are the possible remainders of perfect squares mod 8? 0, 1, & 4

b/c $0^2 \equiv 0 \mod 8$, $1^2 \equiv 1 \mod 8$, $2^2 \equiv 4 \mod 8$, $3^2 \equiv 1 \mod 8$, $4^2 \equiv 0 \mod 8$, & $(8-a)^2 \equiv (-a)^2 \equiv a^2 \mod 8$

3pts c) Deduce from a) & b) what remainders mod 24 could possibly be remainders of perfect squares.

The remainders need to be $\left.\begin{matrix} 0 \text{ or } 1 \mod 3 \\ 0, 1, \text{ or } 4 \mod 8 \end{matrix}\right\}$ 6 combinations.

Any combination can be achieved: 0 1 4 ~~8~~ 9 12 16 ~~17~~ ~~20~~

(crossed out ones are $\equiv 2 \mod 3$) (listed ones have good remainders mod 8)

3pts d) Verify that each of your answers in c) is, indeed, a remainder of a perfect square mod 24.

$0^2 \equiv 0 \mod 24$. $3^2 \equiv 9 \mod 24$

$1^2 \equiv 1 \mod 24$ $4^2 \equiv 16 \mod 24$

$2^2 \equiv 4 \mod 24$ $6^2 \equiv 12 \mod 24$

5pts e) Use the Euclidean algorithm to find gcd(1989, 629).

$1989 = 3 \cdot 629 + 102$ $629 = 6 \cdot 102 + 17$ $102 = 6 \cdot 17 + 0$

$\gcd(1989, 629) = \gcd(629, 102) = \gcd(102, 17) = 17$

5pts f) Find $\gcd(2^5 \cdot 3^4 \cdot 7^2, 3^2 \cdot 7^3 \cdot 11^5)$. You can give its prime factorization - no need to multiply it out.

$3^2 \cdot 7^2$