FINAL: MATH 109, FALL 2011.

No books, calculators, cell-phones, notes or tables are permitted. Good luck !

(1) (10 points) Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

$\gcd(a,b)=1 \Rightarrow \exists x,y\in\mathbb{Z},\ 1=ax+by$

$\Rightarrow c = acx + bc$? $\Rightarrow a|c$.

$a \mid acx$

$a \mid bc$

(2) (a) (3 points) Let $k, l \in \mathbb{N}$. Prove that $2^k - 1|2^l - 1$ if $k|l$.

$k|l \Rightarrow \exists k'\in\mathbb{N},\ l=kk'$ ($k,l\in\mathbb{N}$)

$2^l \overset{2^k-1}{\equiv} 2^{kk'} \equiv (2^k)^{k'} \equiv 1^{k'} = 1.$

$\Rightarrow 2^k-1 \mid 2^l-1.$

Date: 12/5/2011.

(b) (~~15~~ 12 points) Prove that $\gcd(2^n-1, 2^m-1) = 2^{\gcd(n,m)}-1$ for any $m, n \in \mathbb{N}$.

By the part (a), $2^{\gcd(m,n)}-1 \mid 2^m-1$ and $2^{\gcd(m,n)}-1 \mid 2^n-1$.

Therefore $2^{\gcd(m,n)}-1 \le \gcd(2^m-1, 2^n-1) = d$.

Let $a_0 = m$, $a_1 = n$ and

$$a_0 = a_1 \times q_0 + a_2, \quad 0 \le a_2 < a_1$$
$$\vdots$$
$$a_{i-1} = a_i \times q_{i-1} + a_{i+1}, \quad 0 \le a_{i+1} < a_i$$
$$\vdots$$
$$a_{k-1} = a_k \cdot q_{k-1}.$$

By Euclid's algorithm $d = \gcd(m,n) = a_k$.

By induction on i, we prove that $d \mid 2^{a_i}-1$.

Base cases. $d \mid 2^{a_0}-1$ and $d \mid 2^{a_1}-1$ by the definition of gcd.

Induction Step $2^{a_{i-1}} = 2^{a_i q_{i-1} + a_{i+1}} \overset{d}{\equiv} \left(2^{a_i}\right)^{q_{i-1}} \cdot 2^{a_{i+1}}$

By the strong induction hypothesis, we have

$$2^{a_{i-1}} \equiv 2^{a_i} \equiv 1 \pmod{d}.$$

Hence $2^{a_{i+1}} \overset{d}{\equiv} 1$, which proves our claim. Thus

$$\left.\begin{array}{l} d \mid 2^{a_k}-1 = 2^{\gcd(m,n)}-1 \\ 2^{\gcd(m,n)}-1 \le d \end{array}\right\} \Rightarrow d = 2^{\gcd(m,n)}-1.$$

(3) (15 points) For any set X, prove that $|X| < |P(X)|$ where $P(X)$ is the power set of X.

First we notice that $g: X \to P(X)$, $g(x) = \{x\}$ is an injection. Hence $|X| \leq |P(X)|$.

Now we prove any function $f: X \to P(X)$ is NOT onto. Thus there is no bijection from X to $P(X)$. Hence $|X| < |P(X)|$.

Let $A = \{x \in X \mid x \notin f(x)\}$.

Claim $A \notin \mathrm{Im}(f)$.

Pf If not, $A = f(a)$. Now if $a \in A$, then by the definition of A $a \notin f(a) = A$, which is a contradiction. If $a \notin A = f(a)$, then by the def. of A $a \in A$ which is a contradition. This completes the proof of our claim and we are done.

(4) (10 points) Find all the solutions of 106x=6 in $\mathbb{Z}/58\mathbb{Z}$.

$106x = 6$ in $\mathbb{Z}/58\mathbb{Z} \Rightarrow 106x \equiv 6 \pmod{58}$

$\Rightarrow 53x \equiv 3 \pmod{29}$

Euclid's algorithm

$53 = 29 \times 1 + 24$ $\quad 24 = -29 \times 1 + 53$

$29 = 24 \times 1 + 5$ $\quad 5 = -24 \times 1 + 29$

$24 = 5 \times 4 + 4$ $\quad 4 = -5 \times 4 + 24$

$5 = 4 \times 1 + 1$ $\quad 1 = -4 \times 1 + 5$

$4 = 1 \times 4$

$1 = 4 \times 1 + 5$

$= -(-5 \times 4 + 24) + 5 = 5 \times 5 - 24$

$= (-24 \times 1 + 29) \times 5 - 24 = -24 \times 6 + 29 \times 5$

$= -(-29 \times 1 + 53) \times 6 + 29 \times 5 = 29 \times 11 - 53 \times 6$

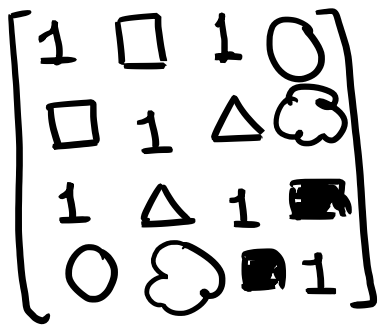
$\Rightarrow -53 \times 6 \overset{29}{\equiv} 1 \Rightarrow x \overset{29}{\equiv} -6 \times 3 = -18 \equiv 11.$

$\Rightarrow x \overset{58}{\equiv} 11 \text{ or } 40 \Rightarrow x = [11] \text{ or } [40].$

(5) (10 points) Let $X = \{1, 2, 3, 4\}$. How many relations R are there on X which satisfy all these conditions: R is reflexive. R is symmetric, and $1R3$? Explain your solution.

Relations are subsets of $X \times X$. So any 4×4 box of 0 and 1 gives us a relation and vice versa. [The (i,j) entry is 1 iff iRj.]

Since R is reflexive, on the diagonal we get 1. The (1,3) & (3,1) are also 1. Because of symmetry



if we know the upper part, the lower part is uniquely determined. Hence we get 2^5 relations.

(6) (10 points) Let $X = \{1, 2, 3, 4, 5, 6, 7\}$. Compute $|\{A \subseteq X | \, |A| \text{ is even}\}|$. Explain your solution. $\{1, 2, \cdots, 2011\}$

Solution 1. Let $P_E(X) = \{A \subseteq X \mid |A| \text{ is even}\}$ and $P_O(X) = \{A \subseteq X \mid |A| \text{ is odd}\}$. It is clear that $f : P_E(X) \longrightarrow P_O(X)$, $f(A) = X \setminus A$ is a bijection. Hence $|P_E(X)| = |P_O(X)|$. On the other hand,

$$2^{2011} = |P(X)| = |P_E(X)| + |P_O(X)| = 2\,|P_E(X)|.$$

Thus $|P_E(X)| = 2^{2010}$.

Solution 2. $|P_E(X)| = \sum_{i=0}^{1005} \binom{2011}{2i}$.

On the other hand, $(x+1)^{2011} = \sum_{j=0}^{2011} \binom{2011}{j} x^j$.

Thus $0 = (-1+1)^{2011} = \sum_{\substack{j=0 \\ 2 \nmid j}}^{2011} \binom{2011}{j} - \sum_{\substack{j=0 \\ 2 \mid j}}^{2011} \binom{2011}{j}$?

and $2^{2011} = (1+1)^{2011} = \sum_{\substack{j=0 \\ 2 \nmid j}}^{2011} \binom{2011}{j} + \sum_{\substack{0 \le j \le 2011 \\ 2 \mid j}} \binom{2011}{j}$

$$\Longrightarrow \sum_{\substack{j=0 \\ 2 \nmid j}}^{2011} \binom{2011}{j} = 2^{2011}/2 = 2^{2010}.$$

(7) (15 points) Let $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f([x]_m) = [12x]_n$. Prove that f is well-defined if and only if $n/\gcd(12, n)$ divides m. What is the necessary and sufficient condition under which f is a bijection?

f is well-defined $\iff$ $\forall x_1, x_2$ $x_1 \overset{m}{\equiv} x_2 \Rightarrow 12x_1 \overset{n}{\equiv} 12x_2$

$\iff \forall x,\ m \mid x \Rightarrow n \mid 12x$

On the other hand $n \mid 12x \iff \frac{n}{\gcd(12,n)} \mid \frac{12}{\gcd(12,n)} x$

$\iff \frac{n}{\gcd(12,n)} \mid x$.

$\iff \frac{n}{\gcd(12,n)} \mid m$

($\Rightarrow$ let $x = m$)

f is a bijection $\iff m = n$ and $f([x]) = [12x]$ is bijective.

$\iff m = n$ and $\gcd(m, 12) = 1$.

(f is bijection iff 12 is a unit iff $\gcd(12, m) = 1$.)

(8) (10 points) Find the remainder of the division of 3^{2011} by 2012.

By Euler's theorem $3^{\varphi(2012)} \equiv 1 \pmod{2012}$

as $\gcd(3, 2012) = 1$.

On the other hand, $\varphi(2012) = \varphi(4 \times 503)$

$= \varphi(4)\varphi(503)$

$= 2 \times 502 = 1004$.

Thus $3^{1004} \equiv 1 \Rightarrow 3^{2011} \equiv 3^{1004 \times 2 + 3}$

$\equiv 3^3 = 27 \ (2012)$.

So the remainder is 27.