Discrete Test 2 Review (answers).

(1) Let $a, b \in \mathbb{Z}$. Prove that if $a \mod 6 = 5$ and $b \mod 4 = 3$ then $4a + 6b \mod 8 = 6$.
(Direct Proof)

Proof. Assume $a = 6m + 5$ and $b = 4k + 3$.
$\Rightarrow 4a + 6b = 4(6m + 5) + 6(4k + 3)$
$= 24m + 20 + 24k + 18$
$= 24m + 24k + 38$
$= 8(3m + 3k + 4) + 6$

□

(2) Suppose we were to prove or find a counterexample to the statement "$\forall x \in S, y \in \mathbb{Z}$, $y \leq 25 \Rightarrow 5|(x + y)$."
(Answer without using the word "not" or the symbol "$\sim$.")

a)For a direct proof we assume $(y \leq 25)$ and show $5|(x + y)$.

b) For proof using the contrapositive we assume $5 \nmid (x + y)$ and show $(y > 25)$.

c) For proof by contradiction we assume
$\exists\, x \in S, y \in \mathbb{Z}$ s.t. $(y \leq 25) \wedge 5 \nmid (x + y)$ and show that we reach a false conclusion.

d) To disprove, using a counterexample, we find:
$\exists$ a specific pair (x, y) with $(x \in S)$ and $(y \in \mathbb{Z})$, $s.t.$ $(y \leq 25) \wedge 5 \nmid (x + y)$.

(3) Let $a_1 = 2, a_2 = 4$, and $a_n = 5a_{n-1} - 6a_{n-2}, n \geq 3$. Prove that $\forall n \in \mathbb{N}, n \geq 3 \Rightarrow a_n = 2^n$ for all natural numbers n.

Base cases:
$n = 1$ Check that the given value $a_1 = 2$ matches the formula $a_1 = 2^1$ (yes).
$n = 2$ Check that the given value $a_2 = 4$ matches the formula $a_2 = 2^2$ (yes).

Induction Assume: $\forall n = 0, \ldots, k, a_n = 2^n$. Specifically, $a_k = 2^k; a_{k-1} = 2^{k-1}; a_{k-2} = 2^{k-2}$; etc.

Show: $a_{k+1} = 2^{k+1}$.

Proof. $a_{k+1} = 5a_{k+1-1} - 6a_{k+1-2}$
$= 5a_k - 6a_{k-1}$
$= 5(2^k) - 6(2^{k-1})$
$= 5(2^k) - 3 \cdot 2(2^{k-1})$
$= 5(2^k) - 3(2^k)$
$= 2(2^k)$
$= 2^{k+1}$ □

(4) Prove that: $\forall a, b \in \mathbb{Z}$, if a is even and b is odd then 4 does not divide $(a^2 + 2b^2)$.

Proof. a) Negate the statement.
Assume $\exists$ a even and b odd, and $4|(a^2 + 2b^2)$.
b) Assuming that negation, prove that 4 divides 2.

Assume $a = 2k$ and $b = 2n + 1$. Also assume $4|(a^2 + 2b^2)$, OR $a^2 + 2b^2 = 4m$, for $m \in \mathbb{Z}$.

Then, by substituting, $4|(4k^2 + 2(4n^2 + 4n + 1))$. OR, by substitution $4k^2 + 2(4n^2 + 4n + 1) = 4m$

Then after algebra we get: $4(m - k^2 - 2n^2 - 2n) = 2$

Therefore $4|2$. (Contradiction) □

(5) Prove that $\sqrt{5}$ is irrational. You may assume that if $5|x^2$ then $5|x$, by the F.T. of arithmetic since 5 is prime.[3]

Proof. Assume the contrary: $\sqrt{5} = \frac{p}{q}$ in lowest terms.
$\Rightarrow q\sqrt{5} = p.$
$\Rightarrow q^2(5) = p^2.$ (*)
$\Rightarrow 5|p^2.$
$\Rightarrow 5|p.$
$\Rightarrow p = 5k.$
$\Rightarrow p^2 = 25k^2.$
$\Rightarrow q^2(5) = 25k^2.$ (by substituting in (*) above.)
$\Rightarrow q^2 = 5k^2.$
$\Rightarrow 5|q^2.$
$\Rightarrow 5|q.$
Contradiction, since $5|p$ and $5|q$ contradicts assumption of lowest terms. □

(6) Prove $\forall n \in \mathbb{Z}, n \geq 2 \Rightarrow \sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Proof. Base case: Let $n = 2$. Then $\sum_{i=1}^{2} i^3 = 1^3 + 2^3 = 9.$

Also $\left(\frac{2(2+1)}{2}\right)^2 = 9.$

Induction: Assume that $\sum_{i=1}^{k} i^3 = \left(\frac{k(k+1)}{2}\right)^2$.

Show that: $\sum_{i=1}^{k+1} i^3 = \left(\frac{(k+1)((k+1)+1)}{2}\right)^2$.

$$\sum_{i=1}^{k+1} i^3$$
$$= \sum_{i=1}^{k} i^3 + (k+1)^3$$
$$= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3$$
$$= \frac{(k(k+1))^2}{4} + \frac{4(k+1)^3}{4}$$
$$= \frac{(k+1)^2(k^2+4(k+1))}{4}$$
$$= \frac{(k+1)^2(k^2+4k+4)}{4}$$
$$= \frac{(k+1)^2(k+2)^2}{4}$$
$$= \left(\frac{(k+1)((k+1)+1)}{2}\right)^2.$$

□

(7) Disprove $\forall n \in \mathbb{N}, (n^2 - n + 5)$ is prime.

Let $n = 10$. Then $n^2 - n + 5 = 95$ which is not prime. (Disproved by counterexample.)

(8) Prove that: $\forall n \in \mathbb{N}$, if $n \geq 2$ then $3|(2^{(4n-4)} + 2^{(2n-3)})$.

Proof. Base case: $n = 2 : 2^4 + 2^1 = 18 = 3(6)$.
Inductive step: Assume true that $3|(2^{(4k-4)} + 2^{(2k-3)})$. Then $(2^{(4k-4)} + 2^{(2k-3)}) = 3m$.
Now show for $n = k + 1 : 3|(2^{(4(k+1)-4)} + 2^{(2(k+1)-3)})$.

$2^{(4(k+1)-4)} + 2^{(2(k+1)-3)} = 16(2^{(4k-4)}) + 4(2^{(2k-3)})$
$= 15(2^{(4k-4)}) + 3(2^{(2k-3)}) + 2^{(4k-4)} + 2^{(2k-3)}$
$= 15(2^{(4k-4)}) + 3(2^{(2k-3)}) + 3m$
$= 3(5(2^{(4k-4)}) + 2^{(2k-3)} + m)$.
$\Rightarrow 3|(2^{(4(k+1)-4)} + 2^{(2(k+1)-3)})$. □

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

(9) Given the one-time-pad sequence $(2, 6, 13, 1)$ encrypt the word COOL. Your output will be letters.

EUBM

(10) Use the BBS sequence to encrypt the word ZAP. Use the seed $a_0 = 11$ and the constant $m = 7 * 13 = 91$.

KES

(11) Use the same BBS sequence to decrypt the word LLJ. Use the seed $a_0 = 11$ and the constant $m = 7 * 13 = 91$.

AHG

(12) Use the same BBS sequence to encrypt the digits 1101.

0110

(13) Use the same BBS sequence to decrypt the digits 1110.

0101

(14) Don't forget to study quizzes!