Math 3613
SOLUTIONS TO FIRST EXAM
9:30 – 10:20 , September 25, 2013

1. Definitions and Axioms (5 pts each)
(a) What is the **Well-Ordering Axiom** for the set $\mathbb{N}$ of non-negative integers?

- Every nonempty subset of $\mathbb{N}$ has a least element.

(b) State the **Division Algorithm** theorem.

- Suppose a, b are integers with $b > 0$. Then there exists unique integers q and r such that

$$a = bq + r \quad , \tag{i}$$
$$0 \leq r < b \quad . \tag{ii}$$

(c) What is the **greatest common divisor** $GCD\,(a, b)$ of two integers a and b. Is $GCD(0, 0)$ defined? Why not?

- The greatest common divisor of two integers a, b not both zero is the integer d such that (i) $d|a$ and $d|b$ and (ii) if c is any integer dividing both a and b then $c \leq d$.

(d) What is the definition of a **prime number**?

- A prime number is an integer p with the property that it has exactly four divisors: 1, -1, p and $-p$.

(e) What is the **contrapositive** of a conditional statement? Give an example.

- The contrapositive of a conditional statement $P \implies Q$ is the conditional statement $not - Q \implies not - Q$.

2. (15 pts) Use Mathematical Induction to prove

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

- When $n = 1$ the proposition says

$$((2)\,(1) - 1) = 1^2$$

which is true as both sides evaluate to 1. We now show that the validity of this proposition at level N implies its validity at level $N + 1$. So assume (*) is true for $n = N$. The corresponding proposition at level $N + 1$ would be

(**) $$1 + 3 + 5 + \cdots + (2N - 1) + (2\,(N + 1) - 1) =^{?} (N + 1)^2$$

The using the validity of (*) at level N we can replace the left hand side with

$$N^2 + (2\,(N + 1) - 1) = N^2 + 2N + 2 - 1 = N^2 + 2N + 1 = (N + 1)^2$$

which agrees with the right hand side of (**). Since the case $n = 1$ is true, and the validity at level N implies the validity at level $N + 1$, the proposition is proved by mathematical induction. ∎

3. (10 pts) Prove that if $a, b, u, v \in \mathbb{Z}$ are such that $au + bv = 1$, then $GCD(a, b) = 1$.

   - *Proof.* Suppose t is a common divisor of a and b. Then $a = tk$ and $b = t\ell$ for some integers k, ℓ. But then
   $$1 = au + bv = (tk)\, u + (t\ell)\, v = t\,(ku + \ell v)$$
   So t divides 1. This means $t \in \{-1, 1\}$, Clearly, the greatest common divisor corresponds to $t = 1$. ∎

4. (10 pts) Let p be prime number. Prove that for any integer a either $GCD(p, a) = 1$ or $p|a$.

   - If p is prime, then by definition its only divisors are $\{-1, 1, p, -p\} = \{-|p|, -1, 1, |p|\}$. Therefore its set of common divisors with any integer a is
   $$\{\text{common divisors of } a \text{ and } p\} = \{\text{divisors of } a\} \cap \{-|p|, -1, 1, |p|\} \subseteq \{-|p|, -1, 1, |p|\}$$
   The greatest common divisor must therefore be either 1 or $|p|$. If $GCD\,(a, p) = 1$, then we're done, as we have fulfilled the conclusion of the proposition. If $CGD\,(a, p) = |p|$, then $|p|$ is a common divisor of a and p; and so p is a divisor of a. So in either case, the conclusion of the proposition is fulfilled. ∎

5. (10 pts) Use the Euclidean algorithm to compute $GCD(42, 144)$.

   -
   $$\begin{aligned} 144 &= (3)\,(42) + 18 \\ 42 &= (2)\,(18) + 6 \\ 18 &= (3)\,(6) + 0 \\ &\Longrightarrow \quad GCD\,(42, 144) = 6 \text{ (the last non-zero remainder)} \end{aligned}$$

6. (10 pts) Let p be an integer with the following property: if $p \mid (ab)$ then $p \mid a$ or $p \mid b$. Prove that p is prime (without using Theorem 7).

- (Proof by contradiction.) Suppose p is not prime. Then it has a factorization

(*) $$p = rs \quad \text{with} \quad 1 < |r|, |s| < |p|$$

On the other hand, since p certainly divides itself, it must also divide the product rs. But then the special property of p requires

$$p \mid (rs) \quad \Longrightarrow \quad p|r \text{ or } p|s$$

If $p|r$ then $|p| \leq |r|$, but that conflicts with the inequality $1 < |r| < |p|$ in (*). Similarly, if $p|s$ then $|p| \leq |s|$, which also conflicts with the inequality $1 < |s| < |p|$ in (*). We conclude no such factorization is possible and so p is prime. ∎

7. (10 pts) Prove that if p is prime and $p|a^n$, then $p^n|a^n$.

- Suppose p is prime and $p|a^n$. Writing $a^n = (a)(a)\cdots(a)$ (i.e writing a^n as a product with n factors of a). Corollary 8 then says p must divide one of the factors a. So $p|a$. If we now write

$$a = kp$$

and raise both sides to the power n we have

$$a^n = (kp)^n = (k^n)\, p^n \quad \Longrightarrow \quad p^n|a^n$$

∎

8. (10 pts) Use the Fundamental Theorem of Arithmetic to prove that there are no nonzero integers a, b for which $a^2 = 2b^2$.

- By the Fundamental Theorem of Arithmetic, both a and b have prime factorizations

$$a = p_1 \cdots p_k \quad , \quad b = q_1 \cdots q_\ell$$

where the number of prime factors (k for a and ℓ for b) is unique. Squaring both a and b,

$$\begin{aligned} a^2 &= (p_1 \cdots p_k)(p_1 \cdots p_k) \\ b^2 &= (q_1 \cdots q_\ell)(q_1 \cdots q_\ell) \end{aligned}$$

we see that a^2 and b^2 have, respectively, $2k$ and 2ℓ prime factors. Now consider the number or prime factors on either side of

$$a^2 = 2b^2$$

The left hand side has $2k$ prime factors, but the right hand side has $2\ell+1$ prime factors (2ℓ coming from b^2 and another prime factor coming from the 2). But we can't have an even number of prime factors on one side and an odd number of prime factors on the other; because the Fundamental Theorem of Arithmetic says the number of prime factors must be unique. We conclude that there are no nonzero integers a, b such that $a^2 = 2b^2$. ∎