15-151 Math Foundations CS – EXCEL

Topic: **Division, Unit, GCD, Euclidean Algo, Bezout's, Coprime, Reverse Euclidean Algo, LCM, Prime, Irreducible, Prime Factorisation, Infinitely Many Primes**

Session Date: **Thu 4 Oct 2018**

EXCEL Leader: Sam Yong
Email: myong@andrew.cmu.edu

Academic Development
Cyert Hall B5 | 412-268-6878

Services available: Supplemental Instruction (SI), Academic Counseling in Study Skills, Individual & Walk-in Tutoring

0. Agenda
   1) Review of basic concepts, definitions, theorems, algorithms (important)
   2) Practice problems on Division & GCD (important)
   3) Practice problems on Euclidean Algorithm (important)
   4) Practice problems on Reverse Euclidean Algorithm (important)
   5) Miscellaneous problems on basic number theory
   6) Problems on Primes (take-home)

"The really unusual day would be one where nothing unusual happens."

– Persi Diaconis

Puzzle 001. You found some lost ancient wisdom. It's the answer to the ultimate question of life, the universe, and everything. But it's written in the convoluted ancient language! What is the answer?

J X U D K C R U H V E H J O J M E

U X U E B H T J B M R D J V W L V H N H O L

FYI

(01, A, 21)	(07, G, 24)	(13, M, 18)	(19, S, 07)	(25, Y, 14)
(02, B, 04)	(08, H, 20)	(14, N, 02)	(20, T, 08)	(26, Z, 06)
(03, C, 19)	(09, I, 05)	(15, O, 12)	(21, U, 13)	
(04, D, 11)	(10, J, 01)	(16, P, 26)	(22, V, 25)	
(05, E, 10)	(11, K, 09)	(17, Q, 03)	(23, W, 15)	
(06, F, 23)	(12, L, 17)	(18, R, 22)	(24, X, 16)	

1. Review of basic concepts, definitions, theorems, algorithms

- Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that ________________________ (Division Theorem). We say _____ is the quotient and _____ is the remainder of _______________ (Definition 3.1.2). We say *b* divides *a*, or that *b* is ____________________, if there exists ____________________ (Definition 3.1.4). To denote the fact that *b* divides *a* we write __________. For the negation statement _______________ we write __________. We say $u \in \mathbb{Z}$ is a unit if __________ (Definition 3.1.7). _____ and _____ are the only units in integers.
- Let $a, b \in \mathbb{Z}$. An integer *d* is a greatest common divisor of *a* and *b* if (a) __________ and __________, and (b) if _________________________ then __________ (Definition 3.1.9). Do NOT use the Euclidean Algorithm to find the following. __________ and __________ are the greatest common divisors of 18 and 42. _____ and _____ are the greatest common divisors of 19 and 57. _____ and _____ are the greatest common divisors of 1 and 42. __________ pair of integers *a*, *b* has a greatest common divisor (Theorem 3.1.12). Let $a, b \in \mathbb{Z}$. An integer *m* is a least common multiple of *a* and *b* if (a) __________ and __________, and (b) if _______________ _______________ then _______________ (Definition 3.1.38).
- Let $a, b, q, r \in \mathbb{Z}$, and suppose that $a = qb + r$. Then $\gcd(a, b) =$ _______________ (Theorem 3.1.17). This is the essential proposition that justifies the Euclidean Algorithm.
- Let $a, b, c \in \mathbb{Z}$, and let $d = \gcd(a, b)$. The equation $ax + by = c$ has a solution $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ if and only if _______________ (Theorem 3.1.22 Bézout's Lemma). By this theorem, does the equation $2x + 3y = 42$ has a solution? __________. The equation $5x + 10y = 97$? __________. Linear Diophantine Equations are equations of the form _______________ where __________.
- Let $a, b \in \mathbb{Z}$. We say *a* and *b* are coprime (or _______________) if _______________. Given *a* and *b* are coprime, if $d \in \mathbb{Z}$ such that *d* | *a* and *d* | *b*, then _______________ (Proposition 3.1.28). Let $a, b, c \in \mathbb{Z}$. If *a* and *b* are coprime and *a* | bc, then _______________ (Proposition 3.1.32).
- Let *p* be a non-zero non-unit. We say *p* is prime if for all __________, if __________ then __________ or __________ (Definition 3.2.1). Let *a* be a non-zero non-unit. We say *a* is reducible if _______________ for some non-units *m*, *n*; otherwise, it is _______________ (Definition 3.2.6). $p \in \mathbb{Z}$ is prime if and only if *p* is __________ (Theorem 3.2.11).

Puzzle 002. Use the four provided numbers and only these operators $(+, -, \times, \div)$ to construct 24.

a. 1, 2, 3, 4

b. 3, 8, 9, 13

---

2. Prove or disprove each of the following statements.
   1) $\gcd(a, b) = \gcd(a, a + b)$
   2) $\gcd(a, b) = \gcd(a, ab)$
   3) $\mathrm{lcm}(a, b) = \mathrm{lcm}(a, a + b)$
   4) $\mathrm{lcm}(a, b) = \mathrm{lcm}(a, ab)$
   5) $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$

3. What is the last digit of $2^{151} \cdot 7^{251}$?

4. Find the greatest common divisors of 42 and 151. Express the positive greatest common divisor as a linear combination of 42 and 151.

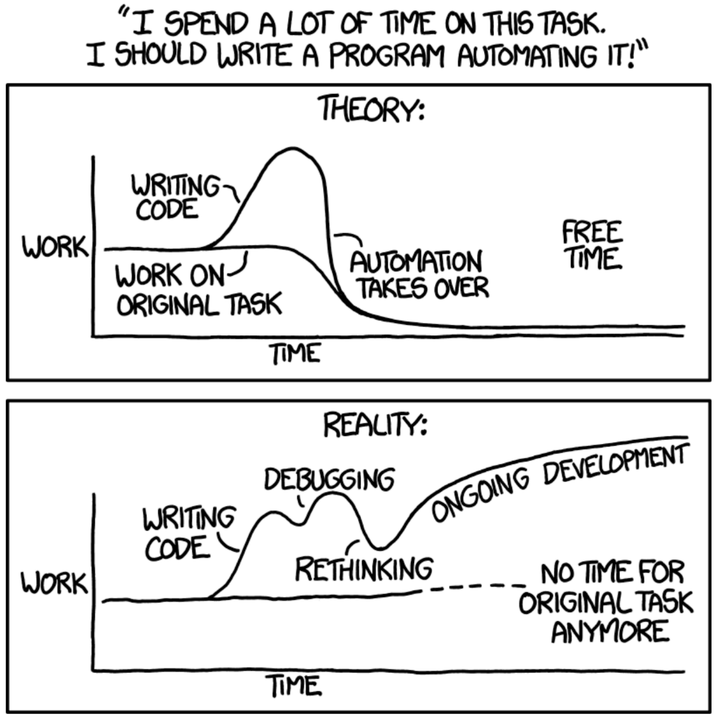
5. Find the greatest common divisors of 273 and 754. Express the positive greatest common divisor as a linear combination of 273 and 754.

6. Find the least common multiples of 273 and 754. (Hint: You can use something you've proven in a previous problem on this handout.)

7. Given arbitrary *n* consecutive integers starting at $m \geq 2$, i.e. consecutive integers $m, m + 1, \ldots, m + n - 1$. Find an integer that is NOT divisible by ANY of the given *n* integers.

8. (Difficult) Let m, n be relatively prime positive integers. Calculate $\gcd(5^m + 7^m, 5^n + 7^n)$.

[Note: If there is no time in the session to go over this problem, do not feel bad if you cannot solve it on your own. This problem was on 1996 Math Olympiads Japan National Contests.]



[The following practice on prime numbers will likely be take-home exercise.]

9. Find the canonical prime factorization for the following numbers.
    1) 111
    2) 151
    3) 1001
    4) 2018
    5) 3628800 (try use the fact that this number is in fact 10!)

10. Let $n \in \mathbb{Z}$ with $n > 2$. Prove that the set $\{k \in \mathbb{Z} \mid n < k < n!\}$ contains a prime number.

11. Prove that $151 \mid \binom{151}{k}$ for any $0 < k < 151$.