18.781 First Midterm

You can use your book “An Introduction to the Theory of Numbers” and your class notes freely. However, you may not consult any other books or sources. To receive full credit you must justify all your steps.

1. (15 points) Find the greatest common divisor of 715 and 1001. Express the greatest common divisor of 715 and 1001 as a linear combination of 715 and 1001. Find the least common multiple of 715 and 1001.

2. (10 points) Find the least positive integer which satisfies the congruences
$x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.

3. (20 points) Find all the solutions of the congruence $x^2 + 27x + 17 \equiv 0 \pmod{375}$.

4. (5 points) Find all the solutions of the congruence $12x \equiv 20 \pmod{16}$.

5. (10 points) Prove that an integer $m > 1$ is a prime if and only if m divides $(m-1)! + 1$.

6. (20 points) Let g, h and n be three positive integers such that $n > g + h$. Prove the identity

$$(-1)^g \binom{n}{g+h}\binom{g+h}{g} = \sum_{k=g}^{n-h} (-1)^k \, 2^{n-k-h} \binom{n}{k}\binom{k}{g}\binom{n-k}{h}$$

(Hint: Use the binomial theorem to express $(x-y)^n$. Then consider $(\frac{\partial}{\partial x})^g(\frac{\partial}{\partial y})^h$.)

7. We say that an integer n can be expressed as sums and differences of the k-th powers of j integers if we can find j integers $x_1, \ldots, x_j$ and appropriate choices of signs so that $n = x_1^k + \cdots x_r^k - x_{r+1}^k \cdots - x_j^k$. For example, $3 = 2^2 - 1^2$, so 3 can be expressed as sums and differences of two squares.

(i) (6 points) Using the identities $2x+1 = (x+1)^2 - x^2$ and $2x = x^2 - (x-1)^2 + 1^2$ show that every integer can be expressed as the sums and differences of three squares. On the other hand, show that 6 cannot be expressed as a sum or difference of only two squares.

(ii) (14 points) Prove that 6 divides $n^3 - n$ for every n. Using the identity $6x = (x+1)^3 + (x-1)^3 - 2x^3$ conclude that every integer can be expressed as sums and differences of the cubes of 5 integers. Considering numbers $9m + 4$ show that a representation cannot be found using less than 4 cubes.

Extra credit (iii) (50 points) In part (ii) do 4 cubes suffice or does one need at least 5? (Hint: Do not attempt this problem before finishing and checking the rest of the exam.)