Problem Set 3 - Thomas Boyko - 30191728

1. (a) Use the Chinese Remainder Theorem to determine all the solutions to $x^2+1 \equiv 0 \pmod{1313}$.
Rework the equation to obatin $x^2 \equiv -1 \pmod{1313}$. So $1313|x^2+1$. Then $101|x^2+1$ and $13|x^2+1$.
Now we are given the modular equations $x^2 \equiv -1 \pmod{101}$ and $x^2 \equiv -1 \pmod{13}$ and if we can solve for both of these squares we can use Chinese Remainder theorem to find the general solution $\pmod{1313}$.
By trial and error we can find: $5^2 \equiv (-5)^2 \equiv -1 \pmod{13}$; as well $10^2 \equiv (-10)^2 \equiv 100 \equiv -1 \pmod{101}$. Convenient!
To use Chinese Remainder Theorem, we can do most of the setup once and extend it to the rest of our cases.

$$\begin{aligned} x &\equiv a \pmod{101} \\ x &\equiv b \pmod{13} \\ m &= 101 \\ n &= 13 \\ t &= 70 \\ s &= 4 \end{aligned}$$

And using $x_0 = sna + tmb$, we can get our four solutions:

$$\begin{aligned} x_0 &= (4)(101)(5) + (70)(13)(10) = 11120 &&\equiv 616 \pmod{1313} \\ x_1 &= (4)(101)(-5) + (70)(13)(10) = 7080 &&\equiv 515 \pmod{1313} \\ x_2 &= (4)(101)(5) + (70)(13)(-10) = -7080 &&\equiv 798 \pmod{1313} \\ x_3 &= (4)(101)(-5) + (70)(13)(-10) = -11120 &&\equiv 697 \pmod{1313} \end{aligned}$$

(b) Is 17 a square modulo 104?
Let $x^2 \equiv 17 \pmod{104}$. Then $104|x^2-17$, so $13|x^2-17$ and $8|x^2-17$. We can transform both of these divisiblilty statements into congruences:
First, $x^2 \equiv 17 \equiv 4 \pmod{13}$. Clearly a solution is given by $x \equiv \pm 2 \pmod{13}$. And since 13 is an odd prime, these are our only solutions.
Next, $x^2 \equiv 17 \equiv 1 \pmod{8}$ Write $8 = 2^3$ and we can see our solutions will be given by ± 1, and $p^{3-1} \pm 1 = 4 \pm 1$. So our solutions to $x^2 \equiv 17 \pmod{8}$ are $-1, 1, 3$, and 5.
Since we have a set of congruences, and $8, 13$ are coprime, we know from Chinese Remainder Theorem that each of these pairs of congruences has a unique solution, and therefore $x^2 \equiv 17 \pmod{104}$ has a solution and 17 is a square mod 104.

2. Let $p = 47$, $q = 59$, $N = pq = 2273$, and $e = 157$.

(a) Compute a multiplicative inverse d, modulo $\phi(N)$.
We must first find $\phi(2273)$ with its prime factorization, $N = 47 \times 59$.

$$\begin{aligned} \phi(N) &= \left(2773\left(1-\frac{1}{47}\right)\left(1-\frac{1}{59}\right)\right) \\ &= 2668. \end{aligned}$$

d, e will be inverses $\pmod{2668}$. So we want to find d so that $157d \equiv 1 \pmod{2668}$. We obtain the Diophantine Equation $157d + 2668y = 1$.
Using the inverse Euclidean Algorithm we obtain $d = 17$. So the inverse of 157 $\pmod{2668}$ is 17.

(b) Every two-letter string (including A-Z and spaces) can be converted to a number-message between 0 and 2626, by replacing a space by 00, A: by 01, B by 02, etc ... For example, ME becomes 1305. Encrypt the two-letter string HI by computing its number-message m, and the ciphertext m^e mod N.
HI becomes 1309, and $1309^{157} \equiv 840 \pmod{2773}$.

(c) Decrypt the sequence of ciphertexts $0802, 2179, 2657, 1024$ to find a message.
We use our decryption key $d = 17$, and $M^d \pmod N$ to find:

$$802^{17} \equiv 2305 \pmod{2773}$$
$$2179^{17} \equiv 1212 \pmod{2773}$$
$$2657^{17} \equiv 269 \pmod{2773}$$
$$1024^{17} \equiv 1405 \pmod{2773}.$$

Some of these numbers do not correspond to letters but the message seems to be WELLB?NE.

3. Prove that if p is a prime and $a \equiv b \pmod{p^2 - p}$, then $a^a \equiv b^b \pmod p$.

Proof. Since $a \equiv b \pmod{p^2 - p}$, $p^2 - p | a - b$. From this we can say that $p|a - b$ and $p - 1|a - b$. So $a \equiv b \pmod p$ and $a \equiv b \pmod{p - 1}$.

From $a \equiv b \pmod{p - 1}$ we can say that $k\phi(p) = a - b$. This allows us to derive:

$$a^{a-b} \equiv a^{\phi(p)k} \equiv a^{\phi(p)^k} \equiv 1^k \equiv 1 \pmod p.$$

And since $a^{a-b} \equiv 1 \pmod p$, $a^a \equiv a^b \pmod p$.

Finally, because $a \equiv b \pmod p$, $a^b \equiv b^b \pmod p$. And therefore, $a^a \equiv b^b \pmod p$. □

4. Let p be a prime. Define the map $v_p : \mathbb{Z}^* \to \mathbb{Z}$ by $v_p(n) = e$, if e is the highest exponent with which p occurs in the factorization of n. For example $v_2(20) = 2, v_5(-20) = 1$ etc. We can extend this map to $v_p : \mathbb{Q}^* \to \mathbb{Z}$ by $v_p(\frac{m}{n}) = v_p(m) - v_p(n)$, where m and n are at lowest terms, i.e. $GCD(m, n) = 1$. For example, for $p = 3$, $v_3(\frac{18}{17}) = 2$ Show that:

(a) $v_p(r \cdot s) = v_p(r) + v_p(s)$ for any $r, s \in \mathbb{Q}^*$.
Let $r, s \in \mathbb{Q}^*$. Write the prime factorizations of r, s:

$$r = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_j}$$
$$s = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_j}.$$

With all $\alpha, \beta \in \mathbb{Z}$ since $r, s \in \mathbb{Q}$. If a prime is not in the prime factorization, then it will simply be raised to the power of 0. Suppose we are taking $v_{p_i}(r)$ for some $1 \le i \le j$. Since a prime can only appear in either the numerator or denominator, we write $v_{p_i}(r) = \alpha_i$, and for s, $v_{p_i}(s) = \beta_i$.
Now we write $rs = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \dots p_r^{\alpha_r+\beta_r}$. Therefore, $v_{p_i}(rs) = \alpha_i + \beta_i = v_{p_i}(r) + v_{p_i}(s)$.

(b) $v_p(r + s) \ge \min\{v_p(r), v_p(s)\}$ for any $r, s \in \mathbb{Q}^*$.
Take the prime factorizations of r, s as in part (a). Again, as above, $v_{p_i}(r) = \alpha_i$ and $v_{p_i}(s) = \alpha_i$, for some $1 \le i \le j$.
Then write:

$$r + s = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_j} + p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_j}$$

. If $\alpha_i < \beta_i$, we can factor out $p_i^{\alpha_i}$, and the opposite holds as well. In other words, we can factor out whichever is lower, $p_i^{\alpha_i}$ or $p_i^{\beta_i}$.
So $r + s$ becomes

$$r + s = p_i^{\min\{\alpha_i,\beta_i\}}(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i - \min\{\alpha_i,\beta_i\}} \dots p_r^{\alpha_j} + p_1^{\beta_1} p_2^{\beta_2} \dots p_i^{\beta_i - \min\{\alpha_i,\beta_i\}} \dots p_r^{\beta_j}).$$

And therefore $v_p(r + s)$ is greater than or equal to $\min\{\alpha_i, \beta_i\}$; $p_i^{\min\{\alpha_i,\beta_i\}}$ is guaranteed to divide $r + s$, but p_i might also divide the other part of our product. Therefore, $v_p(r + s) \ge \min\{v_p(r), v_p(s)\}$

(c) The map v_p is onto
Suppose $y \in \mathbb{Z}$. In order to show that our map is onto, we must show that for any choice of y, we have a choice of r so that $y = v_p(r)$. Simply, we can choose $r = p^y$. Then p^y is the highest exponent of p that appears in the prime factorization of r, and $y = v_p(r)$.
So the map is onto.

5. Define the p-adic absolute value $|.|_p$ as follows : $|.|_p : \mathbb{Q}^* \to \mathbb{R}$, given by, $|q|_p = p^{-v_p(q)}$. In the example above, $v_3(\frac{18}{17}) = 2$ thus, $|\frac{18}{17}| = 3^{-2} = \frac{1}{9}$. Show that,

   (a) $|r+s|_p \leq max\{|r|_p, |s|_p\}$.

   Proof. Let $p \in \mathbb{Z}$ and $r, s \in \mathbb{Q}^*$.
   Consider $|r+s|_p = p^{-v_p(r+s)}$. We know from question 4 b) that $v_p(r+s) \geq \min\{v_p(r), v_p(s)\}$, so $-v_p(r+s) \leq -\min\{v_p(r), v_p(s)\}$.
   From this we can write $p^{-v_p(r+s)} \leq p^{-\min\{v_p(r), v_p(s)\}}$.
   There are two cases. First the case that $v_p(s) \leq v_p(r)$. In this case, $\min\{v_p(r), v_p(s)\} = v_p(s)$. Therefore,

$$|r+s|_p = p^{-\min\{v_p(r), v_p(s)\}} = p^{-v_p(s)} = |s|_p \leq \max\{|r|_p, |s|_p\}.$$

   The other case is where $v_p(r) < v_p(s)$.

$$|r+s|_p = p^{-\min\{v_p(r), v_p(s)\}} = p^{-v_p(r)} = |r|_p \leq \max\{|r|_p, |s|_p\}.$$

   So in either case, $|r+s|_p \leq \max\{v_p(r), v_p(s)\}$. □

   (b) Show that if $r \in \mathbb{Z}$, then $|r|_p \leq 1$. In fact, describe the set $\{r \in \mathbb{Q}^* : |r|_p \leq 1\}$.

   Proof. Let $r \in \mathbb{Z}^*$ in lowest terms, and suppose that p is some chosen prime.
   If p is not in the prime factorization of r, then $v_p(r) = 0$, and $|r|_p = p^{-0} = 1$.
   If p is in the prime factorization, it is raised to some $\alpha \in \{0, 1, \ldots\}$, and $v_p(r) = \alpha$.
   So $|r|_p = p^{-\alpha} = \frac{1}{p^\alpha}$. Since $\alpha \geq 0$, this must be less than or equal to 1. □

   Considering rationals, we see that if p divides the denominator of some $r = \frac{a}{b}$, then $v_p(r)$ will be negative, and so $|r|_p$ will be a prime p to some positive power, which must be ≥ 1.