Basic Number Theory and Modulo Joy
Chapter 3

1. (a) Find integers x and y such that $17x + 101y = 1$
The way that you start this problem is using the Extended Euclidean Algorithim. You can go about that as follows. You can use the Extended Eucleadean algorithm to find s and t of the following equation

$$as + nt = gcd(a, n)$$

. So in our case $a = 17, n = 101, gcd(a, n) = 1$. The first step is to do the Euclidean algorithm in order to find the quotients.

$$\begin{aligned} 101 &= 17 \cdot 5 + 16 \\ 17 &= 16 \cdot 1 + 1 \\ 16 &= 1 \cdot 16 \end{aligned}$$

Our quotients are $5, 1, 16$. The extended Euclidean algorithm gives us a recursion in terms of the quotients q and s, t to find s_n and t_n. That is of the following form

$$\begin{aligned} x_0 = 0, x_1 = 1, x_j &= -q_{j-1}x_{j-1} + x_{j+2} \\ y_0 = 1, y_1 = 0, y_j &= -q_{j-1}y_{j-1} + y_{j+2} \end{aligned}$$

Now knowing this equation we can solve for x_n where n is the last step in the Euclidean Algorithim.

$$\begin{aligned} x_0 &= 0 x_1 = 1 \\ x_2 &= -5 \cdot 1 + 0 \\ x_3 &= -1 \cdot -5 + 1 \end{aligned}$$

Going through these same steps for solving y_n we get $x_n = 6$ and $y_n = -1$. Checking our answer we see that this indeed true.

(b) Find $17^{-1} \pmod{101}$
To find the inverse of $17 \pmod{101}$. We need to find a number x that holds the following condition $17x \equiv 1 \pmod{101}$. If we look close at the equation from part (a). We can write it as the following

$$\begin{aligned} 17x + 101y = 1 & \\ 17x &= 1 - 101y \\ 17 - 1 &= -101y \\ 17 - 1 &= 101 \cdot (-y) \\ 17x &\equiv 1 \pmod{101} \end{aligned}$$

So x is 6 in other words $17^{-1} \pmod{101}$ is 6

2. (a) Solve $7d \equiv 1 \pmod{30}$
Similar to our solution to question 1. We need to use the Euclidean Algorithim to find the quotients then solve for the equation $as + nt = 1$ where $a = 7, n = 30$. Then d will be s.

$$\begin{aligned}30 &= 7 \cdot 4 + 2\\ 7 &= 3 \cdot 2 + 1\\ 3 &= 1 \cdot 3\end{aligned}$$

Now knowing this equation we can solve for x_n where n is the last step in the Euclidean Algorithim.

$$\begin{aligned}x_0 &= 0, x_1 = 1\\ x_2 &= -4 \cdot 1 + 0\\ x_3 &= -3 \cdot -4 + 1\\ x_3 &= 13\end{aligned}$$

So $x_n = 13$, thus d = 13.

3. (a) Find all solutions of $12x \equiv 28 \pmod{236}$
First we start by seeing if the gcd(12,236) is 1. The $gcd(12, 236) = 4$. So in order to find the solution we must divide the equation by the gcd(12,236) if 4 doesent divide 28 then there is no solution. If it does then we solve the reduced equation for x. The resulting equation is:$3x \equiv 7 \pmod{59}$. The gcd(3,59) is 1 so we solve like normal.Since the inverse of $3 \pmod{59}$ is 20 we multiply both sides by 20. Which gives $x \equiv 140 \pmod{59}$.140 Modulo 59 is 22.So $x \equiv 22, 81, 140, 199, 22+59\cdot 5, \ldots$
(b) Find all solutions of $12x \equiv 30 \pmod{236}$. Since 30 is not divisible by 4. There is no solution

11. Let p be prime. Show that $a^p \equiv a \pmod{p}$ for all a. We can show this is true by using Fermat's Theorem. If we have $a^{p-1} \equiv 1 \pmod{p}$. We can multiply by a on both sides to get the formula. $a^p \equiv a \pmod{p}$. This holds for all a.

12. Divide 2^{10203} by 101. What is the remainder?
The question is asking for the remainder after dividing a number which is the same as asking for $2^{10203} \pmod{101}$ First notice that $2^{10203} = 2^{100^{102}} \cdot 2^3$. So we can use Fermats Theorem to simplify $2^{100} \equiv 1 \pmod{101}$. This gives us $1^{102} \cdot 2^3 \pmod{101}$. Which is equal to 8.

13. Find the last 2 digits of 123^{562}. Since we are looking for the last 2 digits of a number that is the same as getting the remainder of dividing by 100.Since 100 is composite we can use Eulers ϕ equation.

$$\phi(100) = 100 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 100 \cdot \frac{4}{10} = 40$$

.So we know that $123^{40} \equiv \pmod{100}$
Using this we can conclude

$$123^{40 \cdot 14} \cdot 123^2 \equiv 1^{14} \cdot 123^2 \equiv 15129 \equiv 29 \pmod{100}$$

. Thus the last two digits are 29.

23. (a) Let $x = b_1 b_2 \ldots b_w$ be an integer written in binary(for example, when $x = 1011$, we have $b_1 = 1$,$b_2 = 0$,$b_3 = 1$,$b_4 = 1$,). Let y and n be integers. Perform the following procedure:

    1. Start with $k = 1$ and $s_1 = 1$.
    2. If $b_k = 1$, let $r_k \equiv s_k y \pmod{n}$ if $b_k = 0$, let $r_k = s_k$.
    3. Let $s_{k+1} \equiv r_k^2 \pmod{n}$
    4. If $k = w$, stop. If $k < w$, add 1 to k and go to (2).

    Show that $r_w \equiv y^x \pmod{n}$

    Proof. In order to prove this we will use induction on the number of steps or iterations, i , taken for $i = w$.
    Base Case: Let i = 1. Then notice that we have $k = 1$ and $s_1 = 1$. Then there are two cases : $b_k = 1$ or $b_k = 0$
    Case 1: If $b_1 = 0$ then $r_1 = s_1$.So

    $$r_1 \equiv y^{b_1} \pmod{n} = 1 \equiv y^0 \pmod{n}$$

    Case 2: If $b_1 = 1$ then $r_1 = s_1 y$.So

    $$s_1 y \equiv y^{b_1} \pmod{n} = 1 \cdot y \equiv y^1 \pmod{n}$$

    Induction Step: Assume that this is true for k iterations. In order to finish the prove we need to show that its true for $k + 1$ iterations.
    Notice in step 3 we have $s_{k+1} \equiv r_k^2 \pmod{n}$. But since we assumed that this is true for k iterations then we have the following:

    $$s_{k+1} \equiv r_k^2 \equiv y^{2b_1 b_2 \ldots b_k} \pmod{n}$$

    So there are two cases now
    Case 1: If $b_{k+1} = 0$ then $r_{k+1} = s_{k+1}$.So

    $$s_{k+1} \equiv y^{b_1 b_2 \ldots b_k} \pmod{n} = y^{2b_1 b_2 \ldots b_k} \equiv y^{2b_1 b_2 \ldots b_k} y^0 \pmod{n}$$

    Case 2: If $b_k = 1$ then $r_{k+1} = s_{k+1} y^{k+1}$.So

    $$y^{2b_1 b_2 \ldots b_k} y^{b_{k+1}} \equiv y^{b_1 b_2 \ldots b_k b_{k+1}} \pmod{n}$$

    $\square$

    (b) Find all solutions of $12x \equiv 30 \pmod{236}$. Since 30 is not divisible by 4. There is no solution