CS 70 Discrete Mathematics and Probability Theory
Summer 2023 Huang, Suzani, and Tausik

# HW 3

## 1 Modular Practice

Note 6

Solve the following modular arithmetic equations for $x$ and $y$.

(a) $9x+5 \equiv 7 \pmod{13}$.

(b) Show that $3x+12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x+4y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2023} \equiv x \pmod{12}$.

(e) $7^{62} \equiv x \pmod{11}$.

**Solution:**

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{13}.$$

Now since $\gcd(9,13) = 1$, 9 has a (unique) inverse mod 13, and since $9 \times 3 = 27 \equiv 1 \pmod{13}$ the inverse is 3. So multiply both sides by $9^{-1} \equiv 3 \pmod{13}$ to get:

$$x \equiv 6 \pmod{13}.$$

(b) Notice that any number $y \equiv 4 \pmod{21}$ can be written as $y = 4+21k$ (for some integer $k$). Evaluating $y$ mod 3, we get $y \equiv 1 \pmod{3}$.

Since the right side of the equation is $1 \pmod{3}$, the left side must be as well. However, $3x+12$ will never be $1 \pmod{3}$ for any value of $x$. Thus, there is no possible solution.

(c) First, subtract the first equation from four times the second equation to get:

$$\begin{aligned} 4(2x+y)-(5x+4y) &\equiv 4(4)-0 \pmod{7} \\ 8x+4y-5x-4y &\equiv 16 \pmod{7} \\ 3x &\equiv 2 \pmod{7} \end{aligned}$$

Multiplying by $3^{-1} \equiv 5 \pmod{7}$, we have $x \equiv 10 \equiv 3 \pmod{7}$.

Plugging this into the second equation, we have

$$2(3)+y \equiv 4 \pmod{7},$$

so the system has the solution $x \equiv 3 \pmod{7}$, $y \equiv 5 \pmod{7}$.

(d) We use the fact that $13 \equiv 1 \pmod{12}$. Thus, we can rewrite the equation as

$$x \equiv 13^{2023} \equiv 1^{2023} \equiv 1 \pmod{12}.$$

(e) One way to solve exponentiation problems is to test values until one identifies a pattern.

$$\begin{aligned}
7^1 &\equiv 7 \pmod{11} \\
7^2 &\equiv 49 \equiv 5 \pmod{11} \\
7^3 &= 7 \cdot 7^2 \equiv 7 \cdot 5 \equiv 2 \pmod{11} \\
7^4 &= 7 \cdot 7^3 \equiv 7 \cdot 2 \equiv 3 \pmod{11} \\
7^5 &= 7 \cdot 7^4 \equiv 7 \cdot 3 \equiv 10 \equiv -1 \pmod{11}
\end{aligned}$$

We theoretically could continue this until we the sequence starts repeating. However, notice that if $7^5 \equiv -1 \implies 7^{10} = (7^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}$.

Similarly, $7^{60} = (7^{10})^6 \equiv 1^6 \equiv 1 \pmod{11}$. As a final step, we have $7^{62} = 7^2 \cdot 7^{60} \equiv 7^2 \cdot 1 = 49 \equiv 5 \pmod{11}$.

## 2 Euler's Totient Function

Note 6

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to $n$ which are relatively prime to it. We develop a general formula to compute $\phi(n)$.

(a) Let $p$ be a prime number. What is $\phi(p)$?

(b) Let $p$ be a prime number and $k$ be some positive integer. What is $\phi(p^k)$?

(c) Show that if $\gcd(a,b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. (Hint: Use the Chinese Remainder Theorem.)

(d) Argue that if the prime factorization of $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.$$

**Solution:**

(a) Since $p$ is prime, all the numbers from 1 to $p-1$ are relatively prime to $p$.

So, $\phi(p) = p - 1$.

(b) The only positive integers less than $p^k$ which are not relatively prime to $p^k$ are multiples of $p$.

Why is this true? This is so because the only possible prime factor which can be shared with $p^k$ is $p$. Hence, if any number is not relatively prime to $p^k$, it has to have a prime factor of $p$ which means that it is a multiple of $p$.

The multiples of $p$ which are $\leq p^k$ are $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. There are $p^{k-1}$ of these.

The total number of positive integers less than or equal to $p^k$ is $p^k$.

So $\phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$.

(c) Let $A$ be the set of positive integers $1 \leq i \leq a$ such that $\gcd(i,a) = 1$, and let $B$ be the set of positive integers $1 \leq j \leq b$ such that $\gcd(j,b) = 1$. Since $\gcd(a,b) = 1$, the Chinese Remainder Theorem gives that every choice $(i,j) \in A \times B$ corresponds with a unique integer $1 \leq k \leq ab$, where $k \equiv i \pmod{a}$ and $k \equiv j \pmod{b}$. Note then that $\gcd(k,a) = \gcd(i,a) = 1$ and $\gcd(k,b) = \gcd(j,b) = 1$. Thus, $\gcd(k,ab) = 1$, so the Chinese Remainder Theorem associates each $(i,j)$ to a unique $1 \leq k \leq ab$ relatively prime to $ab$.

Moreover, note that each $1 \leq k \leq ab$ relative prime to $ab$ can be associated with a unique $(i,j) \in A \times B$ such that $k \equiv i \pmod{a}$ and $k \equiv j \pmod{b}$. Thus, we have a bijection between $A \times B$ and the set of positive integers $1 \leq k \leq ab$ relatively prime to $ab$.

Since $|A| = \phi(a)$, $|B| = \phi(b)$, and the set of positive integers $1 \leq k \leq ab$ relatively prime to $mn$ has cardinality $\phi(ab)$ (by definition), we conclude that $\phi(a)\phi(b) = \phi(ab)$.

(d) Applying part (c) inductively, we conclude that

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \\
&= \prod_{i=1}^{k} \phi(p_i^{e_i}) \\
&= \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1} \\
&= \prod_{i=1}^{k} \frac{p_i - 1}{p_i} p_i^{e_i} \\
&= n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.
\end{aligned}$$

# 3 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if $p$ is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if $p$ is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If $p$ is composite, then it has some prime factor $q$. What can we say about $(p-1)! \pmod{q}$?

**Solution:**

Direction 1: If $p$ is prime, then the statement holds.

For the integers $1, \cdots, p-1$, every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when $x^2 \equiv 1 \pmod{p}$, or when $p \mid x^2 - 1 = (x-1)(x+1)$. Thus, $p \mid x-1$ or $p \mid x+1$, so $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Thus, the only integers from 1 to $p-1$ inclusive whose inverse is the same as itself are 1 and $p-1$.

We reconsider the product $(p-1)! = 1 \cdot 2 \cdots p-1$. The product consists of 1, $p-1$, and pairs of numbers with their inverse, of which there are $\frac{p-1-2}{2} = \frac{p-3}{2}$. The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \equiv -1 \pmod{p}$, as desired.

Direction 2: The expression holds *only if* $p$ is prime (contrapositive: if $p$ isn't prime, then it doesn't hold).

We will prove by contradiction that if some number $p$ is composite, then $(p-1)! \not\equiv -1 \pmod{p}$. Suppose for contradiction that $(p-1)! \equiv -1 \pmod{p}$. Note that this means we can write $(p-1)!$ as $p \cdot k - 1$ for some integer $k$.

Since $p$ isn't prime, it has some prime factor $q$ where $2 \leq q \leq n-2$, and we can write $p = q \cdot r$. Plug this into the expression for $(p-1)!$ above, yielding us $(p-1)! = (q \cdot r)k - 1 = q(rk) - 1 \implies (p-1)! \equiv -1 \pmod{q}$. However, we know $q$ is a term in $(p-1)!$, so $(p-1)! \equiv 0 \pmod{q}$. Since $0 \not\equiv -1 \pmod{q}$, we have reached our contradiction.

# 4 RSA with CRT

Note 7

Inspired by the efficiency of solving systems of modular equations with CRT, Alice decides to use CRT to speed up RSA!

She first generates the public key $(e, N)$ and private key $d$ as normal, keeping track of the primes $pq = N$. Recall that $e$ is chosen to be coprime to $(p-1)(q-1)$, and $d$ is then defined as $e^{-1} \pmod{(p-1)(q-1)}$. Next, she stores the following values:

$$d_p \equiv d \pmod{p-1}$$
$$d_q \equiv d \pmod{q-1}$$

After receiving an encrypted message $c = m^e \pmod{N}$ from Bob, Alice computes the following expressions:

$$x \equiv c^{d_p} \pmod{p}$$
$$x \equiv c^{d_q} \pmod{q}$$

The message $m$ then calculated as the solution to the above modular system.

(a) Show that this algorithm is correct, i.e. that $x \equiv m$ is the only solution $\pmod{N}$ to the above modular system.

(b) Emboldened by her success in using CRT for RSA, Alice decides to invent a new cryptosystem. To generate her keypair, she first generates $N = pq$. Then, she chooses three numbers $g, r_1, r_2$ and publishes the public key $(N, g_1 = g^{r_1(p-1)} \pmod{N}, g_2 = g^{r_2(q-1)} \pmod{N})$. Her private key is $(p, q)$.

To encrypt a message, Bob chooses two numbers $s_1, s_2$ and sends $c_1 = mg_1^{s_1}, c_2 = mg_2^{s_2}$.

Alice decrypts this message by solving the modular system

$$x \equiv c_1 \pmod{p}$$
$$x \equiv c_2 \pmod{q}$$

Show that this algorithm is correct, i.e. show that $x \equiv m$ is the only solution $\pmod{N}$ to the above modular system.

(c) This system is woefully insecure. Show how anyone with access to the public key can recover $p, q$, given that $g_1 \not\equiv 1 \pmod{q}$.

**Solution:**

(a) Intuitively, note that $x = c^{d_p} \equiv m \pmod{p}$, and $x = c^{d_p} \equiv m \pmod{q}$. Therefore, the solution to the modular system must satisfy both constraints, which leaves $m$ as the only solution.

(b) Similarly to the previous question, we have

$$x \equiv mg_1^{s_1} \pmod{p}$$
$$x \equiv mg_2^{s_2} \pmod{q}$$

Key to this subpart is the fact that $g_1^{s_1} = g^{s_1 r_1 (p-1)} \equiv 1 \pmod{p}$, and $g_2^{s_2} = g^{s_2 r_2 (q-1)} \equiv 1 \pmod{q}$. Therefore, this system reduces to

$$x \equiv m \pmod{p}$$
$$x \equiv m \pmod{q}$$

By the previous subpart, we know that $x \equiv m \pmod{N}$.

(c) We are given a value $g_1 = g^{r_1(p-1)} \pmod{p}$ (as part of the public key) that is $1 \pmod{p}$ (by FLT) but not $1 \pmod{q}$. It follows that $g_1 - 1$ is a multiple of $p$, and we can find $\gcd(g_1 - 1, N) = p$. From there, we can find $q = \frac{N}{p}$. Note that if $g_1 \equiv 1 \pmod{q}$, this won't work, since then $g_1 - 1$ is a multiple of $N$ and $\gcd(g_1 - 1, N) = N$. However, then $c_1 = m$ for all encryptions, making it insecure regardless.

# 5 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in GF($p$) for some prime $p \in \mathbb{N}$. We say that two such polynomials $f$ and $g$ are *equivalent* if $f(x) = g(x)$ for every $x \in \text{GF}(p)$.

(a) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over GF(5); then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 70$ over GF(11).

(b) In GF($p$), prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

**Solution:**

(a) Fermat's Little Theorem says that for any nonzero integer $a$ and any prime number $p$, $a^{p-1} \equiv 1 \mod p$. We're allowed to multiply through by $a$, so the theorem is equivalent to saying that $a^p \equiv a \mod p$; note that this is true even when $a = 0$, since in that case we just have $0^p \equiv 0 \pmod{p}$.

The problem asks for a polynomial $\tilde{f}(x)$, different from $f(x)$, with the property that $\tilde{f}(a) \equiv a^5 \mod 5$ for any integer $a$. Directly using the theorem, $\tilde{f}(x) = x$ will work. We can do something similar with $g(x) = 4x^{70} + 9x^{11} + 70$ modulo 11; since $x^{11} \equiv x \pmod{11}$, we can set $\tilde{g}(x) = 4x^{10} + 9x + 4$.

(b) One proof uses Fermat's Little Theorem. As a warm-up, let $d \geq p$; we'll find a polynomial equivalent to $x^d$. For any integer, we know

$$\begin{aligned} a^d &= a^{d-p}a^p \\ &\equiv a^{d-p}a \pmod{p} \\ &\equiv a^{d-p+1} \pmod{p}. \end{aligned}$$

In other words $x^d$ is equivalent to the polynomial $x^{d-(p-1)}$. If $d - (p-1) \geq q$, we can show in the same way that $x^d$ is equivalent to $x^{d-2(p-1)}$. Since we subtract $p-1$ every time, the sequence $d, d-(p-1), d-2(p-1), \ldots$ must eventually be smaller than $p$. Now if $f(x)$ is any polynomial with degree $\geq p$, we can apply this same trick to every $x^k$ that appears for which $k \geq p$.

Another proof uses Lagrange interpolation. Let $f(x)$ have degree $\geq p$. By Lagrange interpolation, there is a unique polynomial $\tilde{f}(x)$ of degree at most $p-1$ passing through the points

$(0, f(0)), (1, f(1)), (2, f(2)), \ldots, (p-1, f(p-1))$, and we designed it exactly so that it would be equivalent to $f(x)$.

# 6 The CRT and Lagrange Interpolation

Note 6
Note 8

Let $n_1, \ldots n_k$ be pairwise co-prime, i.e. $n_i$ and $n_j$ are co-prime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} && (1)\\ x &\equiv a_2 \pmod{n_2} && (2)\\ &\vdots && (\vdots)\\ x &\equiv a_k \pmod{n_k} && (k) \end{aligned}$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

(a) We start by proving the $k = 2$ case: Prove that we can always find an integer $x_1$ that solves $(1)$ and $(2)$ with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer $x_2$ that solves $(1)$ and $(2)$ with $a_1 = 0, a_2 = 1$.

(b) Use part (a) to prove that we can always find at least one solution to $(1)$ and $(2)$ for any $a_1, a_2$. Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.

(c) Now we can tackle the case of arbitrary $k$: Use part (b) to prove that there exists a solution $x$ to $(1)$-$(k)$ and that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$.

(d) For polynomials $p_1(x)$, $p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \bmod q(x)$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.

Define the polynomials $x - a$ and $x - b$ to be co-prime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing $x, a_i$ and $n_i$ with polynomials (using the definition of co-prime polynomials just given), show that the system of congruences

$$\begin{aligned} p(x) &\equiv y_1 \pmod{(x - x_1)} && (1')\\ p(x) &\equiv y_2 \pmod{(x - x_2)} && (2')\\ &\vdots && (\vdots)\\ p(x) &\equiv y_k \pmod{(x - x_k)} && (k') \end{aligned}$$

has a unique solution $\pmod{(x - x_1) \cdots (x - x_k)}$ whenever the $x_i$ are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properties are satisfied.

**Solution:**

(a) Since $\gcd(n_1, n_2) = 1$, there exist integers $k_1, k_2$ such that $1 = k_1 n_1 + k_2 n_2$. Setting $x_1 = k_2 n_2 = 1 - k_1 n_1$ and $x_2 = k_1 n_1 = 1 - k_2 n_2$ we obtain the two desired solutions.

(b) Using the $x_1$ and $x_2$ we found in Part (a), we show that $a_1 x_1 + a_2 x_2 \pmod{n_1 n_2}$ is a solution to the desired equivalences:

$$a_1 x_1 + a_2 x_2 \equiv a_1 \cdot 1 + a_2 \cdot 0 \equiv a_1 \pmod{n_1}$$
$$a_1 x_1 + a_2 x_2 \equiv a_1 \cdot 0 + a_2 \cdot 1 \equiv a_2 \pmod{n_2}.$$

Such result is also unique. Say that we have two difference solutions $x = c$ and $x = c'$, which both satisfy $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$. This would give us $c \equiv c' \pmod{n_1}$ and $c \equiv c' \pmod{n_2}$, which suggests that $(c - c')$ is divisible by $n_1$ and $n_2$. Since $n_1$ and $n_2$ are coprime, $gcd(n_1, n_2) = 1$, $(c - c')$ is divisible by $n_1 n_2$. Writing it in modular form gives us $c \equiv c' \pmod{n_1 n_2}$. Therefore, all the result is unique with respect to $\pmod{n_1 n_2}$

(c) We use induction on $k$. Part (b) handles the base case, $k = 2$. For the inductive hypothesis, assume for $k \leq l$, the system $(1)$-$(k)$ has a unique solution $a \pmod{n_1 \cdots n_k}$. Now consider $k = l + 1$, so we add the equation $x \equiv a_{l+1} \pmod{n_{l+1}}$ to our system, resulting in

$$x \equiv a \pmod{n_1 \cdots n_l}$$
$$x \equiv a_{l+1} \pmod{n_{l+1}}.$$

Since the $n_i$ are pairwise coprime, $n_1 n_2 \cdots n_l$ and $n_{l+1}$ are coprime. Part (b) tells us that there exists a unique solution $a' \pmod{n_1 \cdots n_l n_{l+1}}$. We conclude that $a'$ is the unique solution to $(1)$-$(l+1)$, when taken $\pmod{n_1 n_2 \cdots n_l n_{l+1}}$.

(d) We only need to check that $q_i(x) = (x - x_i)$ and $q_j(x) = (x - x_j)$ are coprime whenever $x_i \neq x_j$; that is, that they don't share a common divisor of degree 1. If $d_i(x) = a_i x + b_i$ is a divisor of $q_i(x)$, then $q_i(x) = q'(x)(a_i x + b_i)$ for some polynomial $q'(x)$. But since $q_i(x)$ is of degree 1, $q'(x)$ must be of degree 0 and hence a constant, so $d_i(x)$ must be a constant multiple of $q_i(x)$. Similarly, any degree 1 divisor $d_j$ of $q_j(x)$ must be a constant multiple of $q_j(x)$, and if $x_i \neq x_j$, then none of these multiples overlap, so $q_i(x)$ and $q_j(x)$ are coprime.

From our result in part (d), the congruences $(1')$-$(k')$ assert that we are looking for a polynomial $p(x)$ such that $p(x_i) = y_i$. The CRT then establishes the existence of $p(x)$, and that it is unique modulo a degree $k$ polynomial. That is, $p(x)$ is unique if its degree is at most $k - 1$. Lagrange interpolation finds $p(x)$.

# 7 Trust No One

Note 8

Gandalf has assembled a fellowship of nine peoples to transport the One Ring to the fires of Mount Doom: five humans, two hobbits, one elf, and one dwarf. The ring has great power that may be of use to the fellowship during their long and dangerous journey. Unfortunately, the use of its

immense power will eventually corrupt the user, so it must not be used except in the most dire of circumstances. To safeguard against this possibility, Gandalf wishes to keep the instructions a secret from members of the fellowship. The secret must only be revealed if enough members of the fellowship are present and agree to use it.

Gandalf has hired your services to help him come up with a secret sharing scheme that accomplishes this task, summarized by the following points:

- There is a party of five humans, two hobbits, an elf, and a dwarf, and a secret message that must remain unknown to everyone if not enough members of the party agree.
- A group of people consisting of at least two people from different people classes and at least one people class that is fully represented (i.e., has all members present) can unlock the secret of the ring.

A few examples: only five humans agreeing to use the ring is not enough to know the instructions. One hobbit and four humans is not enough. However, all five humans and one hobbit agreeing is enough. Both hobbits and the dwarf agreeing is enough.

**Solution:**

**Solution 1**

There will be two parts to this secret: a unanimity secret $U$ and a multi-people secret $M$. $U$ ensures that at least all members of one peoples are in agreement while $M$ ensures that members of at least two peoples are in agreement.

The high-level idea is that the secret of the ring requires both the unanimity and multi-people conditions to be satisfied, so we encode the original secret in a polynomial $R(x)$ determinable by the two values $U$ and $M$; each of $U$ and $M$ themselves are encoded within polynomials as independent secrets determinable when the unanimity and multi-people conditions, respectively, are satisfied. Thus, once both $U$ and $M$ are recovered, they can then be combined to reveal the original secret, since each will be a point of the degree-1 polynomial $R(x)$ whose y-intercept contains the secret of the ring.

We will now detail $U$ and $M$ in order below.

The *unanimity secret* involves creating a separate secret for each people. We will require all members of that people to join forces in order to reveal the secret. For example, the humans will each have distinct points of a degree-4 polynomial and the hobbits will each have distinct points of a degree-1 polynomial. When all members of a people come together, they will reveal $U$ (encoded, for example, as the y-intercept of each of these polynomials). Note that the elf and the dwarf each know $U$ already since they are the only members of their people.

The *multi-people secret* involves creating a degree-1 polynomial $P_m(x)$ and giving one point to all members of each people. For example, the hobbits may each get $P_m(1)$ while the elf gets $P_m(2)$ and the humans each get $P_m(3)$. In this way if members of any two peoples are in agreement, they can reveal $M$ (encoded, for example, as the y-intercept of $P_m(x)$).

Once $U$ and $M$ are each known, they can be *combined* to determine the final secret. $U$ and $M$ allow

us to uniquely determine $R(x)$ and thus $R(0)$, the secret of the ring.

This scheme is an example of hierarchical secret sharing. Let's work out a specific example.

**Example:** Suppose the secret is $s = 4$, $M = 3$, and $U = 2$. From now on, we can work in GF(7) since $s < 7$ and $n < 7$ ($n$ is the number of people who have pieces of the secret).

First we need to create a degree-1 polynomial $R(x)$ such that $R(0) = s = 4$, $R(1) = M = 3$, and $R(2) = U = 2$. By inspection, $R(x) = 6x + 4$ has these properties (e.g. $R(1) = 6 \cdot 1 + 4 = 10 \equiv 3$).

Now we can create the multi-people secret $M$. We choose degree-1 polynomial $P_m(x) = x + 3$ and tell each hobbit $P_m(1) = 4$, the elf $P_m(2) = 5$, each of the humans $P_m(3) = 6$, and the dwarf $P_m(4) = 7 \equiv 0$. Now any two members of distinct peoples can determine $P_m(x)$ and thus $P_m(0)$ by interpolating their two values.

When creating the unanimity secret $U$, we first note that each of the dwarf and the elf will be told $U$ directly since they are the only members of their respective people. On the other hand, the hobbits will each have a point on the degree-1 polynomial $P_{hobbits}(x)$. Suppose $P_{hobbits}(x) = 2x + 2$. Then the first hobbit receives $P_{hobbits}(1) = 4$ and the second receives $P_{hobbits}(2) = 4 + 2 = 6$. When they interpolate using these values, they will discover the original polynomial and therefore $P_{hobbits}(0) = U = 2$. The humans will have a similar secret but with a degree-4 polynomial.

Now suppose that two hobbits and one human come together. The two hobbits work together to determine $U$ as described above. Together the three of them also know $P_m(3) = 6$ and $P_m(1) = 4$, from which they can find $P_m(x)$ and thus $P_m(0) = M = 3$. Now that they have $U$ and $M$, they can interpolate to find $R(x)$ and thus $R(0) = s = 4$.

**Solution 2**

Alternatively, we can construct a single degree 8 polynomial (which requires 9 points to interpolate) and distribute 1 point to each human, 4 points to each hobbit, 8 points to the elf, and 8 points to the dwarf. We can see that if all the humans agree, they will need 4 more points in order to interpolate successfully and each member of all the other peoples are given at least 4 points. Moreover, each of the other peoples have 8 points in total, meaning that if all the hobbits, the elf, or the dwarf agree, they'll only need one more point which can be provided by any additional member of the party outside their people. On the other hand, the most amount of points that could be obtained from an agreeing group that does not satisfy the requirements would be 8, from the group consisting of one hobbit and all but one of the humans. This would be insufficient to interpolate the polynomial so the scheme fulfills the requirements.