Problem Set 0

PAWS 2025

Nathaniel Hurst

1

The Euclidean algorithm computes the greatest common divisor of two positive integers $a > b$ by the following procedure: Use division with remainder to write

$$a = q_1 b + r_1,$$

where the remainder r_1 satisfies $0 \leq r_1 < b$ and q_1 is the quotient. If $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. Otherwise, we can continue, using b as the new dividend and r_1 as the new divisor, and obtain a new remainder $0 \leq r_2 < r_1$. We continue until $r_{k+1} = 0$, in which case $r_k = \gcd(a, b)$.

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_k \cdot r_k \end{aligned}$$

(a) Use the Euclidean algorithm to compute $\gcd(30030, 257)$. Use your result and the fact that

$$30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$$

to prove that 257 is prime.

(b) Use the Euclidean algorithm to compute $\gcd(4883, 4369)$. Use your work to factor 4883 and 4369 into a product of primes.

(a)

$$\begin{aligned} 30030 &= 257(116) + 218 \\ 257 &= 218(1) + 39 \\ 218 &= 39(5) + 23 \\ 39 &= 23(1) + 16 \\ 23 &= 16(1) + 7 \\ 16 &= 7(2) + 2 \\ 7 &= 2(3) + 1 \\ 2 &= 2(1) + 0 \end{aligned}$$

Thus $\gcd(30030, 257) = 1$, or they are coprime. Now observe that since $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ we have that 257 is coprime to all of these factors. Now if 257 was not prime it would have at least two prime factors, but the next prime number after 13 is 17, and $17^2 = 289 > 257$, and since any prime factorization of 257 contains only prime numbers greater than or equal to 17, we must have that 257 is prime.

(b)

$$4883 = 4369(1) + 514$$
$$4369 = 514(8) + 257$$
$$514 = 257(2) + 0$$

Thus $\gcd(4883, 4369) = 257$, and since by the first part of the problem we have that 257 is prime we must have that the prime factorization of these numbers boils down to the prime factorization of their quotients when divided by 257. Thus $4883 = 257(19)$ and $4369 = 257(17)$ are the prime factorizations of these numbers.

2

The **extended Euclidean algorithm** uses the sequence of quotients $q_1, q_2, ..., q_{k-1}$ obtained from the Euclidean algorithm to compute two integers x, y such that $ax + by = \gcd(a, b)$, by forming the two sequences:

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

Then $ax_k + by_k = \gcd(a, b)$.

(a) Show that if there exist integers x and y such that $ax + by = 1$, then $\gcd(a, b) = 1$.

(b) Show that a is invertible mod b if and only if $\gcd(a, b) = 1$. ("Invertible mod b" means there exists an integer z space (mod b) such that $az \equiv 1 \pmod{b}$. We denote $z \pmod{b}$ by $a^{-1} \pmod{b}$.)

(c) Use the extended Euclidean algorithm to compute x and y such that $17x + 101y = 1$. What is $17^{-1} \pmod{101}$?

(a) Let $d = \gcd(a, b)$, then $d \mid a$ and $d \mid b$, or $a = dk_1$ and $b = dk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Thus $1 = ax + by = dk_1x + dk_2y = d(k_1x + k_2y)$, or $d \mid 1$. Thus $d = 1$.

(b) Observe that for the forward direction $az \equiv 1 \pmod{b} \implies az + by = 1$ for some $y \in \mathbb{Z}$, and hence by the previous problem $\gcd(a, b) = 1$. For the converse if $\gcd(a, b) = 1$ then by the extendend Euclidean algorithm there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$, and observing this relation modulo b we have $ax \equiv 1 \pmod{b}$.

(c) First we compute the sequence of quotients by the Euclidean algorithm.

$$101 = 17(5) + 16$$
$$17 = 16(1) + 1$$
$$16 = 1(16) + 0$$

Then we can use the extended Euclidean algorithm to find integers x, y such that $17x + 101y = 1$. Since $16 = 17 - 1$ we have that

$$101 = 17(5) + (17 - 1) \implies 101 = 17(6) - 1 \implies 1 = 17(6) + 101(-1)$$

Then observing this relation modulo 101 we have $17(6) \equiv 1 \pmod{101}$, or $17^{-1} \equiv 6 \pmod{101}$.

3

The Chinese Remainder Theorem states that if $\gcd(n, m) = 1$ and a, b are integers, then there is a unique solution $x \pmod{mn}$ to the simultaneous congruence,

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

(a) Show with a counterexample that the theorem is no longer true if the condition $\gcd(n, m) = 1$ is dropped.

(b) Solve the simultaneous congruence

$$x \equiv 2 \pmod{17}$$
$$x \equiv 9 \pmod{101}$$

(Hint: You could start listing numbers which are congruent to $9 \pmod{101}$, but here's another approach using the work you've already done: Write $x = 17k + 2$, and solve for k in the congruence $17k + 2 \equiv 9 \pmod{101}$)

(a) Observe that for $x \equiv 0 \pmod{2}$ and $x \equiv 0 \pmod{4}$ we have that $x \equiv 4, 0 \pmod{8}$ are both solutions.

(b) We use the hint and write $x = 17k + 2$ and then solve the congruence $17k + 2 \equiv 9 \pmod{101}$. We have $17k \equiv 7 \pmod{101}$, and by part (c) of problem 2 we have $17^{-1} \equiv \pmod{101}$. Thus we have $k \equiv 42 \pmod{101}$ giving us one solution $x \equiv 17(42) + 2 \equiv 716 \pmod{1717}$.

4

Recall that a **group** is a set S together with a binary operation $m : S \times S \longrightarrow S$, such that

(i) for all $s_0, s_1, s_2 \in S$, $m(s_0, m(s_1, s_2)) = m(m(s_0, s_1), s_2)$, (ii) there exists $s^* \in S$ such that $m(s, s^*) = m(s^*, s) = s$ for all $s \in S$, and (iii) for all $s \in S$ there exists $s^{-1} \in S$ such that $m(s, s^{-1}) = m(s^{-1}, s) = s^*$.

We think of m as being a (not necessarily commutative!) multiplication on S, s^* as being a multiplicative identity, and (as the notation indicates) s^{-1} as being the multiplicative inverse of s, and will usually denote m as a product. When the operation m is commutative, we will sometimes denote it with $+$. In this exercise we will recall the basic properties of groups with an emphasis on examples that will be useful in this course.

(a) Prove that the identity element in any group is unique. Prove that each element of a group has a **unique** multiplicative inverse (this justifies the notation s^{-1} used above).

(b) Let G be a group and $g \in G$. Show that the function $m_g : G \longrightarrow G$ defined by $m_{g(h)} = hg$ is a bijection.

(c) Let $GL_2(\mathbb{R})$ denote the set of 2×2 matrices with real entries and determinant 1. Show that $GL_2(\mathbb{R})$ is a group under multiplication. Is $GL_2(\mathbb{R})$ commutative?

(d) Let $\mathbb{Z}/p\mathbb{Z}$ be the set of integers modulo p, i.e., the equivalence classes of the integers under the equivalence relation $a \sim b$ if and only if $p \mid (a - b)$. We define addition and multiplication on $\mathbb{Z}/p\mathbb{Z}$ by $[a] + [b] := a + b \pmod p$ and $[a][b] := ab \pmod p$ (we will usually drop the brackets, but it will be understood that we are multiplying equivalence classes). Prove that $\mathbb{Z}/p\mathbb{Z}$ together with the operation of addition is a group. Prove that $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} - \{[0]\}$ is a group under multiplication.

(e) Is the set $\mathbb{Z}/15\mathbb{Z} - \{[0]\}$ a group under multiplication? Can you identify the maximal subset of $\mathbb{Z}/15\mathbb{Z}$ that is a group under multiplication?

(f) The number of integers less than or equal to N that are coprime to N is denoted by $\varphi(N)$. The function φ is called Euler's phi function,'' or sometimes Euler's totient function.'' Prove that

$$\varphi(N) = N \cdot \prod_{(p \mid N, p \text{ prime})} \left(1 - \tfrac{1}{p}\right)$$

(Hint: One way is to proceed as follows, first show the result when N is a power of a prime. Next show that $\varphi(mn) = \varphi(m)\varphi(n)$ when m and n are relatively prime. Finally, put the two steps together for the general result.

(a) Let $s, s' \in G$ be two identity elements. Then $s = m(s, s') = s'$. Similarly let $s_1, s_2 \in G$ be two multiplicative inverses for an element $s \in G$, and denote the identity element by s^*. Then $s_1 = m(s^*, s_1) = m(m(s_2, s), s_1) = m(s_2, m(s, s_1)) = m(s_2, s^*) = s_2$.

(b) Observe that this function is injective, as if $m_{g(h_1)} = m_{g(h_2)}$ then $h_1 g = h_2 g$, and multiplying by g^{-1} on the right on both sides gives us $h_1 = h_2$. Similarly if $s \in G$ then $m_{g(sg^{-1})} = sg^{-1}g = s$, and so this function is surjective, and hence bijective.

(c) First observe that this set is certainly closed under multiplication for if $A, B \in GL_2(\mathbb{R})$ we have $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$. Now let $A, B, C \in GL_2(\mathbb{R})$. Then each encodes an invertible linear map from $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$. Now since composition of linear maps is associative, so is matrix multiplication. Similarly for the identity element we take the identity matrix I with 1 along the diagonal and 0 otherwise. This matrix has determinant 1 and $AI = IA = A$ for all $A \in GL_2(\mathbb{R})$. Finally using the inverse matrix formula we have that if $A \in GL_2(\mathbb{R})$ with

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$A^{-1} = \frac{1}{\det(A)} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

which has determinant $da - bc = ad - bc = 1$.

This group is not commutative, and here is a counterexample:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(d) First we can verify that this addition is well defined. Let $[a] = [a']$, then $p|(a - a')$, and so $[a + b] = [a' + b]$ as $a + b - a' - b = a - a'$ is divisible by p. Now observe that this addition is associative, as $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = ([a] + [b]) + [c]$ similarly the class of $[0]$ acts as an identity element and every element is invertible as $[a] + [-a] = [a - a] = [0]$. Thus $(\mathbb{Z}/p\mathbb{Z}, +)$ is a group. Now restrict that set to the numbers which are invertible moduluo p under multiplication. We see that multiplication is well defined for if $[a] = [a']$ we have $p|(a - a')$, and so $[ab] = [a'b]$ as $ab - a'b = b(a - a')$ is divisible by p (as $a - a'$ is). Then similarly if a, b are inverible modulo p then ab is, as $ab\mathtt{b}^{-1}a^{-1} \equiv 1 \pmod{p}$. Now observe that this multiplication is associative as $([a][b])[c] = [ab][c] = [abc] = [a][bc] = [a]([b][c])$. Similarly every element is invertible as we restricted the set $\mathbb{Z}/p\mathbb{Z}$ to just the invertible elements under multiplication. Finally $[1]$ acts as an identity element. Thus $(\mathbb{Z}/p\mathbb{Z})^*$ is a group with this multiplication.

(e) $\mathbb{Z}/15\mathbb{Z} - \{0\}$ is not a group under multiplication, for $[3]$ is not invertible as $(3)(5) \equiv 0 \pmod{15}$, and $(0)n \equiv 0 \pmod{15}$ for all n. The maximal subset of $\mathbb{Z}/15\mathbb{Z} - \{0\}$ which is a group under multiplication is the group of units $(\mathbb{Z}/15\mathbb{Z})^*$, as if $a, b \in (\mathbb{Z}/15\mathbb{Z})^*$ then $(ab)b^{-1}a^{-1} \equiv 1 \pmod{15}$ and so $ab \in (\mathbb{Z}/15\mathbb{Z})^*$. Any larger subset contains elements which are not invertible, and hence that larger subset cannot be a group.

(f) First let z be a power of a prime. Then $z = p^n$ for some n. Then the amount of numbers which can be coprime to p^n and less than p^n are exactly $p^n -$ numbers who are a multiple of p, and there are exactly $p^{\{n-1\}}$ such numbers $\{p, 2p, ..., p^2, 2p^2, ..., (p-1)p^{n-1}\}$, thus the amount of numbers less than and coprime to p^n is exactly $p^n - p^{n-1} = p^{n\left(1-\frac{1}{p}\right)}$.

Now observe that when m and n are coprime we have that they share no prime factors, and so

$$\varphi(mn) = mn \cdot \prod_{(p \mid mn, p \text{ prime})}\left(1 - \tfrac{1}{p}\right) = mn \cdot \prod_{(p \mid m, p \text{ prime})}\left(1 - \tfrac{1}{p}\right)\prod_{(p \mid n, p \text{ prime})}\left(1 - \tfrac{1}{p}\right) = \varphi(m)\varphi(n)$$

Then combining this with our previous result we have that for any $x \in \mathbb{Z}_{\geq 2}$ we take the prime factorization $x = p_1^{\alpha_1}...p_n^{\alpha_n}$ and then apply our result to split φ across the prime factors (they are prime and hence coprime) and then we can apply our result to each factor as it is a power of a prime, proving the theorem.

5

Euler's Theorem states that for any integer a coprime to N, $a^{\varphi(N)} \equiv 1 \pmod{N}$.

(a) Prove Euler's Theorem. Use the group theory fact that the order of an element divides the order of the group, applied to the group of integers mod N which are coprime to N under multiplication, $(\mathbb{Z}/N\mathbb{Z})^*$.

(b) Compute $7^{-1} \pmod{30}$ using the extended Euclidean algorithm.

(c) Suppose for some unknown integer m (mod 31), you are given the value of $m^7 \pmod{31}$. How can you find m? (Raise m^7 to a certain power mod 31 and use Euler's Theorem.)

(a) Let $a \in \mathbb{Z}$ be coprime to N. Then the order of a in the group $(\mathbb{Z}/N\mathbb{Z})^*$ divides the order of the group itself, with the order of the group of units being $\varphi(N)$. Then if the order of a is n then $n \mid \varphi(N)$, and so $\varphi(N) = nk$ for some $k \in \mathbb{Z}$, and thus $a^{\varphi(N)} \equiv a^{nk} \equiv 1^k \equiv 1 \pmod{N}$.

(b) First we compute the sequence of quotients using the Euclidean algorithm.

$$30 = 7(4) + 2$$
$$7 = 2(3) + 1$$
$$2 = 1(2) + 0$$

Thus $\gcd(30, 7) = 1$, and so 7 is invertible modulo 30. Then since $2 = 30 - 7(4)$ we have that

$$7 = (30 - 7(4))(3) + 1 \implies 7 = 30(3) - 7(12) + 1 \implies 1 = 7(13) + 30(-3)$$

Now observing this relation modulo 30 we have $7(13) \equiv 1 \pmod{30}$, or $7^{-1} \equiv 13 \pmod{30}$.

(c) Since 31 is prime, all integers less than 31 are coprime to it, and thus we can apply Euler's with $\varphi(31) = 30$, and so

$$\left(m^7\right)^{13} \equiv m^{91} \equiv m^{90}m \equiv \left(m^{30}\right)^3 m \equiv 1^3 m \equiv m \pmod{31}$$

.

6

A **group homomorphism** is a function $\varphi : G \longrightarrow H$, where G and H are groups, such that

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$. In this question we will prove some basic facts about group homomorphisms.

(a) Let 1 be the multiplicative identity in G. Prove that $\varphi(1)$ is the multiplicative identity in H.

(b) For any $g \in G$, show that $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(c) A subgroup of a group is a subset that is also a group under the same operation. Prove that $\varphi(G)$ is a subgroup of H.

(d) The **kernel** of a group homomorphism is the set of elements $g \in G$ such that $\varphi(g) = 1$. We denote this by $\ker(\varphi)$. Prove that $\ker(\varphi)$ is a subgroup of G with the additional property that $g\ker(\varphi)g^{-1} = \ker(\varphi)$ for all $g \in G$. Such a subgroup is called a **normal** subgroup of G.

(e) Let $G/\ker(\varphi)$ denote the set of equivalence classes of G under the equivalence $g \sim h$ iff $gh^{-1} \in \ker(\varphi)$. Define a multiplication on $G/\ker(\varphi)$, and prove that your multiplication is well-defined and makes $G/\ker(\varphi)$ into a group.

(a) Let $h \in \mathfrak{I}(\varphi)$ then $h = \varphi(g)$ for some $g \in G$. Then $\varphi(1)h = \varphi(1)\varphi(g) = \varphi(1g) = h$ (and similarly for $h\varphi(1) = h$). Then if $1'$ is the multiplicative identity of H we have $\varphi(1)h = 1'h \implies \varphi(1)hh^{-1} = 1'hh^{-1} \implies \varphi(1)1' = 1'1' \implies \varphi(1) = 1'$.

(b) Observe that $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. Where $\varphi(1) = 1' \in H$. Thus $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(c) Observe that $\varphi(G)$ is associative under multiplication (due to its elements being part of H, whose elements are associative under multiplication), has an identity element ($\varphi(1) = 1' \in H$), and every element $\varphi(g)$ has inverse $\varphi(g^{-1})$ (by part b). Then it suffices to show that $\varphi(G)$ is closed under multiplication. Let $\varphi(g_1), \varphi(g_2) \in \varphi(G)$, then $\varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) \in \varphi(G)$.

(d) Observe that $\ker(\varphi)$ is associative under multiplication (due to its elements being part of G, whose elements are associative under multiplication), has an identity element 1 (since $\varphi(1) = 1' \in H$ we have $1 \in \ker(\varphi)$), and every element $k \in \ker(\varphi)$ has inverse $k^{-1} \in G$ and $\varphi(k^{-1}) = \varphi(k)^{-1} = 1^{-1} = 1$, and hence $k^{-1} \in \ker(\varphi)$. Then it suffices to show that $\ker(\varphi)$ is closed under multiplication. Let $k_1, k_2 \in \ker(\varphi)$, then $\varphi(k_1k_2) = \varphi(k_1)\varphi(k_2) = (1)(1) = 1$, and hence $k_1k_2 \in \ker(\varphi)$. Thus $\ker(\varphi)$ is a subgroup of G.

Now fix some $g \in G$ Let $k \in g\ker(\varphi)g^{-1}$ then $k = gk_1g^{-1}$ for some $k_1 \in \ker(\varphi)$. Then $\varphi(k) = \varphi(g^{-1}k_1g) = \varphi(g^{-1})\varphi(k_1)\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1$. Thus $k \in \ker(\varphi)$, or $g^{-1}\ker(\varphi)g \subset \ker(\varphi)$. Now let $r \in \ker(\varphi)$. Then by the same reasoning as the previous inclusion $g^{-1}rg \in \ker(\varphi)$, and thus $gg^{-1}rgg^{-1} = r \in g\ker(\varphi)g^{-1}$, or $\ker(\varphi) \subset g\ker(\varphi)g^{-1}$. Thus $\ker(\varphi) = g\ker(\varphi)g^{-1}$.

(e) We define multiplication of equivalence classes as $[g_1][g_2] = [g_1g_2]$. To see that this makes sense, let $[g_1] = [g_{1'}]$ and fix $[g_2]$ then $g_1g_{1'}^{-1} \in \ker(\varphi)$, and $[g_1g_2] = [g_{1'}g_2]$, for $g_1g_2(g_{1'}g_2)^{-1} =$

$g_1 g_2 g_2^{-1} g_{1'}^{-1} = g_1 g_{1'}^{-1} \in \ker(\varphi)$. Observe that this operation is associative, as $[g_1]([g_2][g_3]) = [g_1][g_2 g_3] = [g_1 g_2 g_3] = [g_1 g_2][g_3] = ([g_1][g_2])[g_3]$. Similarly the identity element is $[1]$ as $[g][1] = [g] = [1][g]$. Finally every element is invertible, as $[g][g^{-1}] = [gg^{-1}] = [1] = [g^{-1}g] = [g^{-1}][g]$. Thus $G/\ker(\varphi)$ is a group with multiplication defined thusly.

7

Square and Multiply for Modular Exponentiation ():

```
1  Input: Integers x, e, n
2  Output: x^e (mod n)
3  Convert e to binary: e = (e_k e_{k-1} ... e_0)_2
4  let result ⟵ 1
5
6  from k down to 0:
7      result ⟵ result² mod n
8      if e_i = 1:
9          result ⟵ (result · x) mod n
10     end if
11
12 end for
13 return result
```

(a) Calculate $23^{71} \pmod{31}$ using the square-and-multiply method (showing at most 7 squarings and 4 multiplications).

(b) Given that a multiplication costs $O(n^{\log 3})$ (Karatsuba), what is the expected runtime of the square-and-multiply method?

(a) The binary representation of 71 is $(e_6 e_5 ... e_0)_2 = 1000111$. Now let result = 1. Then since $e_6 = 1$ we do result ⟵ result^2 = $1 \pmod{31}$ and result ⟵ result dot x = $23 \pmod{31}$. Now since $e_5, e_4, e_3 = 0$ we do result ⟵ result^2 = $2 \pmod{31}$, result ⟵ result^2 = $4 \pmod{31}$, and result ⟵ result^2 = $16 \pmod{31}$. Now since $e_2 = 1$ we do result ⟵ result^2 = $8 \pmod{31}$ and result ⟵ result dot x = $29 \pmod{31}$. Similarly since $e_1 = 1$ we do result ⟵ result^2 = $4 \pmod{31}$, and result ⟵ result dot x = $30 \pmod{31}$. Finally since $e_0 = 1$ we do result ⟵ result^2 = $1 \pmod{31}$ and result ⟵ result dot x = $23 \pmod{31}$. Which gives us the result $23^{71} \equiv 23 \pmod{31}$ using 7 squarings and 4 multiplications.

(b) Since multiplication costs $O(n^{\log 3})$ and the maximum number of multiplications corresponds to the number of 1's in the binary expansion of the exponent e, which has $\lfloor \log_2(e) \rfloor + 1$ entries, we must have that the time complexity of the square and multiply method is $O(n^{\log 3} \log_2(e))$.

8

Some cryptographic computations need to calculate values of the form $x^e y^f \pmod{n}$. Devise an efficient algorithm (as an adaptation of Algorithm 1) that outputs $x^e y^f \pmod{n}$ for given integers x, y, e, f, n. (Your algorithm should be able

to compute, for example, $x^{22}y^{13} \pmod n$ in at most 4 multiplications and 4 squarings, plus one precomputation).

Square and Multiply for Modular Exponentiation ():

```
1  Input: Integers x, e, y, f, n
2  Output: x^e y^f (mod n)
3  Convert e and f to binary: e = (e_k e_{k-1} ... e_0)_2, f = (f_r f_{r-1} ... f_0)_2
4  let result ← 1
5
6  from i = max{k, r} down to 0:
7      result ← result² mod n
8      if (e_i, f_i) = (1, 1):
9          result ← (result · xy) mod n
10     else if (e_i, f_i) = (1, 0):
11         result ← (result · x) mod n
12     else if (e_i, f_i) = (0, 1):
13         result ← (result · y) mod n
14     end if
15
16 end for
17 return result
```

You may notice that this algorithm computes $x^{22}y^{13}$ in 5 multiplications and 5 squarings (due to the binary expansion of 22 being 10110), however we can make this 4 squarings and 4 multiplications by including a precomputation which checks the $\max\{k, r\}$ entry of each binary expansion (if one is of less length then its $\max\{k, r\}$ entry is 0) and initializing result based on this entry (for example if $\left(e_{\max\{k,r\}}, f_{\max\{k,r\}}\right) = (1, 1)$ we intialize result as result $\leftarrow xy \pmod n$). Then in the main algorithm we can start at the $\max\{k, r\} - 1$ position, shortening our computation within the acceptable boundaries.