Practice Number Theory Problems

Problem 3-1. GCD

(a) Compute $\gcd(85, 289)$ using Euclid's extended algorithm. Then compute x and y such that $85x + 289y = \gcd(85, 289)$.

Recall Euclid's extended algorithm:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ &\ldots \\ r_{n-1} &= r_n q_{n+1} + r_{n+1}. \end{aligned}$$

We stop when we reach a remainder of 0, that is, when $r_{n+1} = 0$. We obtain $\gcd(a, b) = r_n$.

Fact 1 *For all $a, b \in \mathbb{N}$, if $\gcd(a, b) = d$, then there exists $x, y \in \mathbb{Z}$ such that $ax + by = d$.*

To compute x and y from Fact 1, we can use Euclid's extended algorithm above: starting from r_n, we iterate backwards, by expressing r_n in terms of r_i, a and b, for i decreasing until r_n is expressed in terms of a and b only, as in the example below.

Let's apply Euclid's extended algorithm to compute $\gcd(289, 85)$.

$$\begin{aligned} 289 &= 85 \cdot 4 + 34 \\ 85 &= 34 \cdot 2 + 17 \\ 34 &= 17 \cdot 2 + 0 \end{aligned}$$

The gcd is the last remainder, non-zero: 17. Let's now work backwards and compute x and y:

$$17 = 85 - 34 \cdot 2 = 85 - (289 - 85 \cdot 4) \cdot 2 = 85 - 289 \cdot 2 + 85 \cdot 8 = 85 \cdot 9 - 289 \cdot 2,$$

and thus $x = 9$ and $y = -2$.

(b) Show that if $k \mid mn$, but $\gcd(m, k) = 1$ then $k \mid n$.

Let's first argue intuitively: since k divides m and n and k has no factors in common with m, it must be that all factors of k divide n and hence k divides n.

Let's prove this statement formally: $k \mid mn$ implies that

$$\exists\ q \text{ s.t. } mn = kq. \tag{1}$$

Since $\gcd(m, k) = 1$, we know by Fact 1 that there exists x, y s.t. $mx + ky = 1$ and therefore $m = (1 - ky)/x$.

By replacing m in Eq. (1), we obtain $n(1 - ky) = xkq$ and thus $n = nky + xkq = k(ny + xq)$ so $k \mid n$.

Someone asked me in recitation if it is ok that k is multiplied by a term containing n: the term $(ny + xq)$. The reason this is fine is that all we need from $ny + xq$ is to be an integer, which it is because all of $n, y, x, q \in \mathbb{Z}$. Then, we get that n equals k times some integer, which means that n is a multiple of k.

(c) Show that if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$.

Let $d = \gcd(m, n)$. We know that $d \mid m$ and $d \mid n$ so $d \mid m - n$. Indeed, d is now a common divisor of $m - n$ and n.

To show that d is the largest such divisor, assume by contradiction that it is not the largest divisor. That is, assume that there exists a divisor $d' > d$ such that $d' \mid m - n$ and $d' \mid n$. This means that $d' \mid m$ and that $\gcd(m, n) \geq d' > d$, which achieves a contradiction.

(d) Show that $\gcd(m, n)$ is a linear combination of m and n. Write 1 as a linear combination of 18 and 31.

The first part of this problem follows trivially from Fact 1.

The second part just involves computing the Euler's extended algorithm:

$$\begin{aligned}
31 &= 18 \cdot 1 + 13 \\
18 &= 13 \cdot 1 + 5 \\
13 &= 5 \cdot 2 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

Working backwards (the first equality of each line indicates a substitution from the equations above):

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (5 - 3) = 3 \cdot 2 - 5 \\
&= (13 - 5 \cdot 2) \cdot 2 - 5 = 13 \cdot 2 - 5 \cdot 5 \\
&= 13 \cdot 2 - (18 - 13) \cdot 5 \\
&= 13 \cdot 7 - 18 \cdot 5 \\
&= (31 - 18) \cdot 7 - 18 \cdot 5 \\
&= 31 \cdot 7 - 18 \cdot 12.
\end{aligned}$$

(e) Show that if $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$ then $\gcd(a, mn) = 1$.

Recall that

> **Fact 2** *For all $a, b \in \mathbb{N}$, for all $x, y \in \mathbb{Z}$, if $ax + by = d$, then $\gcd(a, b) \mid d$.*
>
> *Proof.* The proof of this fact is easy. Let $d^* = \gcd(a, b)$. Since $d^* \mid a$ and $d^* \mid b$, it means that $d^* \mid ax + by = d$.

Since $\gcd(a, m) = 1$, by Fact 1, we have that there exists x, y such that $ax + my = 1$. Thus $my = 1 - ax$. Similarly, there exists v and w such that $av + nw = 1$ and thus $nw = 1 - av$.

Therefore, we obtain that $my \cdot nw = (1 - ax)(1 - av)$ and therefore $mn \cdot yw + a(v + x - avx) = 1$, which by Fact 2, gives us that $\gcd(m, n) \mid 1$ so $\gcd(m, n) = 1$.

Problem 3-2. Modular arithmetic

(a) Show that if $a \equiv b \mod n$, then for all integers c, $a + c \equiv b + c \mod n$.

Since $a \equiv b \mod n$, there exists $q \in \mathbb{Z}$ such that $a = b + nq$. This means that $a + c = b + c + nq$. If we compute mod n on both sizes, nq cancels out and we obtain $a + c \equiv b + c \mod n$.

(b) Show that if $a \equiv b \mod n$, then for all positive integers c, $ac \equiv bc \mod n$.

Since $a \equiv b \mod n$, there exists $q \in \mathbb{Z}$ such that $a = b + nq$. This means that $ac = (b + nq)c$. If we compute mod n on both sizes, nqc cancels out and we obtain $ac \equiv bc \mod n$.

(c) Show that if a and n are relatively prime, then there is an integer a' such that $aa' \equiv 1 \mod n$.

By Fact 1, we know that there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Taking mod n on both sides, we obtain $ax \equiv 1 \mod n$.

(d) Show that if a and n are not relatively prime, then a has no multiplicative inverse modulo n.

Let's proceed by contradiction: assume that a has an inverse mod n, denoted a'. Then $aa' \equiv 1 \mod n$, which means that there exists q such that $aa' = nq + 1$ and thus $aa' - nq = 1$. Let $d \neq 1$ be a divisor of a and n. This means that $d \mid aa' - nq$, but $aa' - nq = 1$, so $d \mid 1$ which is a contradiction.

Problem 3-3. Euclid's Algorithm, Inverses, and Fermat's Little Theorem

Recall

Theorem 1 (Fermat's Little Theorem) *If p is prime, then for all $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \mod p$.*

(a) Find the gcd(13, 5) using Euclid's extended algorithm.

$$\begin{aligned} 13 &= 5 \cdot 2 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Thus $\gcd(13, 5) = 1$, which is of no surprise, but we can use the equations above to determine: x and y such that $13x + 5y = 1$.

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3) = 3 \cdot 2 - 5 = (13 - 5 \cdot 2) \cdot 2 - 5 \\ &= 13 \cdot 2 - 5 \cdot 5. \end{aligned} \tag{2}$$

(b) Using your results from (a), what is 5^{-1} modulo 13?

Therefore, $5^{-1} \equiv -5 \mod 13$ because we can apply $\mod 13$ in Eq. (2). We also know that $-5 \equiv 8 \mod 13$, so $5^{-1} \equiv 8 \mod 13$.

(c) Compute $3^{61} \mod 7$ (use Fermat's Little Theorem).

Using Fermat's little theorem, we know that $3^{7-1} \equiv 1 \mod 7$. Therefore, $3^6 \equiv 1 \mod 7$ and hence $3^{60} \equiv 1 \mod 7$. Therefore, $3^{61} \equiv 3^{60} \cdot 3 \equiv 3 \mod 7$.

(d) Can you apply Fermat's Little Theorem to compute $4^{61} \mod 16$?

No, because Fermat's little theorem is only guaranteed to hold modulo a prime and 16 is not a prime.

Problem 3-4. Order of Group Elements

(a) What is the order of 5 in $\mathbb{Z}_{13}^*$?

$$5^1 = 5$$
$$5^2 = 12 \mod 13$$
$$5^3 = 8 \mod 13$$
$$5^4 = 1 \mod 13$$

Order is thus 4.

(b) Find an element of order 3 mod 7.

Try out a few values

$1^3 = 1$, $2^3 \mod 7 = 1$: thus 2 has order 3 mod 7.

Problem 3-5. Generators

(a) Find a safe prime ≥ 20 and it's corresponding Sophie-Germain prime.

Recall that a safe prime p is a prime such that $p = 2q + 1$ where q is a prime. q is called a Sophie-Germain prime.

$p = 23$ and $q = 11$.

(b) Find a generator of $\mathbb{Z}_{11}^*$ - note that 11 is a safe prime, so you should be able to do this by hand!

All you need to try is whether the generator to the power of the factors of $p - 1$ ($p = 11$ here) is not one. If $g^x \equiv 1 \mod p$ for $x < p - 1$, g cannot be a generator because it has shorter cycles than $p - 1$ and thus cannot generate all $p - 1$ values.

$$2^5 = 32 \neq 1 \mod 11.$$

$$2^2 \equiv 4 \neq 1 \mod 11.$$

(c) Test 3 is a generator for $\mathbb{Z}_7^*$ by computing only two exponentiations.

$3^2 \equiv 2 \mod 7 \neq 1$

$3^3 \equiv 6 \mod 7 \neq 1$.

Problem 3-6. Discrete log and related assumptions

(a) Compute the discrete $\log_3 2$ mod 7.

$3^x \equiv 2 \mod 7$. $x = 2$.

(b) Prove that if the Computational Diffie-Hellman assumption is hard, then Discrete Log assumption is also hard.

It is enough to prove the counterpositive: if we can break DL, then we can break CDH.

To break CDH, we are given g^a, g^b and we need to compute ab. Since we know how to break DL, we can compute a and b and then we just multiply them. So we can break CDH.

Problem 3-7. Quadratic Residue

(a) Find Q_7, the set of quadratic residues mod 7.

$$
\begin{aligned}
1^2 &= 1 \mod 7\\
2^2 &= 4 \mod 7\\
3^2 &= 2 \mod 7\\
4^2 &= 2 \mod 7\\
5^2 &= 4 \mod 7\\
6^2 &= 1 \mod 7
\end{aligned}
$$

Therefore, $Q_7 = \{1, 2, 4\}$.