Discussion 3

February 22, 2019

1 Modular Arithmetic

1.1 Translation of Modular Field to Integer Field

When giving proof in modular field, one of the general approaches is to translate modular field $\mathbb{Z}/n\mathbb{Z}$back to integer field $\mathbb{Z}$. That is to say, given $a \equiv b \mod n$, we write $a = b + kn$ where k is an integer. Then we are allow to work in integer the way we are used to to complete the proof.

1.2 Translation of Integer Field back to Modular Field

When we talk about some integers in the form $a = b + kn$, we may think of it as $a \equiv b \mod n$, which is the reverse of translation above. Take a second look at the worksheet problem "prove that every prime number $m > 3$ is either of the form $6k + 1$ or $6k - 1$ for some integer k". What we did was examining case by case when n is congruent to $0, 1, 2, 3, 4, 5$ in this module field.

Example

How many solutions are there to $ax \equiv b \mod n$ in general, where a, b, n are integer constants and x is to be solved?

Solution

We write, as stated above, $ax = b + kn$ where k is an integer. Let $d = \gcd(a, n), a = d\alpha, n = d\beta$ where α, β are coprime based on definition of gcd.
Then $ax = b + kn$ can be written as $d\alpha x = b + kd\beta$. **We can just ignore the module field from now because we already translated modular field back to expression on integers.** This is the whole point about the translation!
Rearrange the equation gives $b = d(\alpha x - k\beta)$. For there to be a solution x, it must be that b is divisible by d. Thus we have a conclusion here:

1. If b is not divisible by d (this is either true of false because b, d are constants, not variables), then there is no solution.

2. If, however, b is indeed divisible by d then how many solutions are there?
   We write b as $b = d\gamma = d(\alpha x - k\beta)$ i.e. $\gamma = \alpha x - k\beta$, where $x \in \{0, 1, \ldots, n-1\}$.
   Thus all solution x to the original equation must satisfies $\alpha x \equiv \gamma \mod \beta$, or equivalently $x \equiv \alpha^{-1}\gamma \mod \beta$ because α and β are coprime and thus α^{-1} exists.
   Now going back to the original equation where we solve for x. Let $x_0 = (\alpha^{-1}\gamma) \mod \beta)$. We know $x_0 \in \{0, 1, \ldots, \beta - 1\}$. Then $x_0, 2x_0, \ldots, dx_0$ are all the possible values for x because $dx_0 \leq d(\beta - 1) \leq n - 1$ but $(d+1)x_0 \geq n$. Thus there are exactly d solutions where $d = \gcd(a, n)$.

Notably, the result still holds even when $d = 1$ i.e. a, n are coprime and there is exactly one solution. To recap, we just proved a claim worth remembering:
For equation $ax \equiv b \mod n$, and $d = \gcd(a, n)$, there is no solution if $b \not\equiv 0 \mod d$, and there are d solutions if $b \equiv 0 \mod d$.

2 Bijection

Lemma

Given function $f : X \to Y$, the following two statements are equivalent:

1. f is bijective.
2. f has an inverse function.

Proof

1. bijective $\Rightarrow$ inverse:
   High level speaking, since f is bijective, we know $\forall y \in Y$ there is exactly one $x \in X$ such that $f(x) = y$. Define $g : Y \to X$ such that g sends y to the corresponding x where $f(x) = y$.
   You can verify that:
   (a) g is a well defined function on Y (meaning $\forall y \in Y$, $g(y)$ is defined).
   (b) $g(f(x)) = x$.
   (c) $f(g(y)) = y$.

   We just found the inverse of f, so the proof is done.

2. inverse $\Rightarrow$ bijective:
   Let g be the inverse function of f. Then by the definition of inverse, $g(f(x)) = x$ and $f(g(y)) = y$.
   Proving bijective is equivalent to proving surjective and injective.
   (a) $\forall y \in Y$, $f(g(y)) = y$, thus y lies in the image of f. By definition, f is surjective.

(b) $\forall x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then we want to show that $x_1 = x_2$. (This is a common way to show injectiveness). Indeed since we have the inverse function g, $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Thus f is injective.