Christian Rudder CS235: pset-1, Section 1 #2, 7, 11, 14 (Due: September 12th):

Exercise 1.2. Let n be a composite integer. Show that there exists a prime p dividing n, with $p \leq n^{1/2}$.

Proof: Let n be a composite integer $\therefore n = ab$ for some integers $a, b \mid 1 < a, b < n$. $a, b \leq n^{1/2}$ must hold, or else $ab > n$. For lost of generality, let $a \leq b$.

$n > 0 \therefore n$ can factor to powers of primes p (Fundamental Theorem of Arithmetic). If p is a composite, factor again until a single prime p' is found. $p' \mid a$ or b then $p' \mid n$ and $p' \leq n^{1/2}$. ■

Theorem 1.5. Let $a, b \in \mathbb{Z}$ with $b > 0$, and let $x \in \mathbb{R}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $r \in [x, x + b)$.

Exercise 1.7. Show that Theorem 1.5 also holds for the interval $(x, x + b]$. Does it hold in general for the intervals $[x, x + b]$ or $(x, x + b)$?

Proof: Thm. 1.5 is the division algorithm, for $a, b \in \mathbb{Z}$ with $b > 0$, and let $x \in \mathbb{R}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $r \in [x, x + b)$.

r, the remainder demonstrates the interval $[x, x + b)$. This interval represents the residue class of a modulo b with shifts in mind. This class is of length b. The question of whether the interval $(x, x+b]$ holds is if it sustains the same length of b to represent the residue classes, which it does.

The intervals $[x, x + b]$ and $(x, x + b)$ do not hold such lengths. ■

Exercise 1.11. Let n be an integer. Show that if a, b are relatively prime integers, each of which divides n, then ab divides n.

Proof: Let a, b be relatively prime integers, then there exists s, t such that $as + bt = 1$. If $a \mid n$ then $n = ak$ for some integer k. If $b \mid n$ then $n = bq$ for some integer q. $n = ak = bq$, multiplying both equations $(ak)(bq) = (ak)(bq) = (ab)(kq)$, kq is some integer say j. Therefore $ab(j) = n$ and $ab \mid n$. ■

Exercise 1.14. Let p be a prime and k an integer, with $0 < k < p$. Show that the binomial coefficient

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

which is an integer (see §A2), is divisible by p.

Proof: The binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is an integer, which when expanded:

$$\frac{p(p-1)...(p-k+1)}{k!}$$

$(p-1)...(p-k+1)$ is some integer m. So $\frac{pm}{k!}$ then $p \mid pm$, p divides the numerator. Since k is less than p, p does not divide $k!$. Therefore k won't cancel the p in the numerator. Since the result is an integer, a factor of p must still be present. ■