ITCS 531: NT4 homework solutions

Rob Egrot

NT4 Q1

Let $p = 11$ and $q = 13$. Choose suitable e and d for use in RSA encryption.

- Choose e.g. $e = 7$.
- d is inverse of e mod 120 (turns out to be 103).
- Can find d with brute force as 120 is a small number (best use a computer).
- Or can implement extended Euclidean algorithm.
- Can also find with a little trick - see the solutions.

NT4 Q2

Prove that if $a \equiv_n b$ then $a^k \equiv_n b^k$ for all $k \in \mathbb{N}$.

- Induct on k. If $k = 0$ then its obviously true as $1 = 1$.
- Suppose it's true for $k - 1$.
- Then $a^k = a.a^{k-1}$ and $b^k = b.b^{k-1}$.
- By assumption we have $a \equiv_n b$.
- By the inductive hypothesis we have $a^{k-1} \equiv_n b^{k-1}$.
- Proposition 2.8(2) applies and tells us that $a^k \equiv_n b^k$ too.

NT4 Q3

Let a and b be coprime. Prove that if $a|c$ and $b|c$ then $ab|c$.

- By Bézout's identity there are x and y with $xa + yb = 1$.
- So $cxa + cyb = c$.
- Also, as $a|c$ there is k with $ak = c$, and as $b|c$ there is l with $bl = c$.
- So, we have $(bl)xa + (ak)yb = c$.
- Rearranging this gives $(ab)(xl + yb) = c$.
- This means $ab|c$ as claimed.

NT4 Q4(a)

Let $n_1, \dots, n_k \in \mathbb{N}$ all be greater than 1 and such that n_i and n_j are coprime for all $i \neq j$. Define $N = \prod_{i=1}^{k} n_i$. For each $i \in \{1, \dots, k\}$ let $a_i \in \{0, \dots, n_i - 1\}$.

a) Let x and y be integers with $x \equiv_{n_i} a_i$ and $y \equiv_{n_i} a_i$ for all i. Prove that $x \equiv_N y$.

- As $\equiv_n$ is transitive, we have $x \equiv_{n_i} y$ for all i.
- So $n_i | (x - y)$ for all i.
- By coprimality and Q3 we have $N | (x - y)$, so $x \equiv_N y$.

NT4 Q4(b)

b) Find $z \in \mathbb{Z}$ with $z \equiv_{n_1} a_1$ and $z \equiv_{n_2} a_2$.

- By Bézout take x, y with $1 = xn_1 + yn_2$.
- So $xn_1 = 1 - yn_2$ and $yn_2 = 1 - xn_1$.
- Define $z = xn_1 a_2 + yn_2 a_1$.
- Then $z = a_2(1 - yn_2) + yn_2 a_1 \equiv_{n_2} a_2$.
- Similarly $z \equiv_{n_1} a_1$.

NT4 Q4(c)

c) Extend part b) to prove that there is z with $z \equiv_{n_i} a_i$ for all $i \in \{1, \ldots, k\}$.

- Induct on k. Trivial when $k = 1$. Let $k > 1$ and suppose true for $k - 1$.
- Define $N' = \prod_{i=1}^{k-1} n_i$.
- By inductive hypothesis, there is $0 \leq z' < N'$ with $z' \equiv_{n_i} a_i$ for all $1 \leq i < k$.
- Then n_k and N' are coprime, because if p is prime and $p|N'$ then $p|n_i$ for some $i < k$, and thus $p \nmid n_k$.
- So by b) there is z with $z \equiv_{N'} z'$ and $z \equiv_{n_k} a_k$.
- Since $z \equiv_{n_i} z' \equiv_{n_i} a_i$, we can use this z.