Discrete Maths

Proof

Just apply the techniques from the lectures, it should come out in the end. Honestly, there aren't really questions that are just about proof. It's simply the framework everything else is built on. If the logic gets confusing, just do the really rigorous stuff, fully writing out the `Assume` and `RTP` (required to prove) and then it should come out quite easily once you follow it step-by-step. The tricky part is mainly the other stuff.

Numbers

Divisibility

Exam tips: simply use the definitions, those usually help if you don't remember identities and stuff like that.

Euclid's Lemma

$$\forall p \in \mathbb{P} \,.\, p \mid ab \implies p \mid a \lor p \mid b \qquad (1.1)$$

Generalised to:

$$k \mid nm \land \gcd(k, n) = 1 \implies k \mid m \qquad (1.2)$$

Proof simply by using $m = m \gcd(k, n)$ and then gcd identities and the definition of 'divides'.

Moduli

Here, you can use the definitions for the simpler stuff, but

Fermat's Little theorem (FLT)

$$\forall p \in \mathbb{P} \,.\; n^p \equiv n \pmod{p} \qquad (2.1)$$

And if $n \not\equiv 0 \pmod{p}$:

$$\forall p \in \mathbb{P} \,.\; n^{p-1} \equiv 1 \pmod{p} \qquad (2.2)$$

So for $\mathbb{Z}_p$ $(0..p-1)$, each number has a modular additive inverse, written by abuse of notation as $n^{-1} \pmod{p}$:

$$\forall n \in \mathbb{Z}_p \,.\, n^{p-2} \equiv n^{-1} \pmod{p} \qquad (2.3)$$

gcds

Basics

Remember these rules - they are ***very*** useful for proving stuff with `gcds`:

1. $\gcd(n, m) = \gcd(m, n) \qquad (3.1)$
2. $\gcd(\gcd(l, n), m) = \gcd(l, \gcd(n, m)) \qquad (3.2)$
3. $\gcd(lm, ln) = l \gcd(m, n) \qquad (3.3)$

Also, if you have $gcd(a, b)$, it's often useful to insert it into any other part of a gcd expression and then use these. You can use this trick for so so so many things, it makes things so much easier!

Also remember from (one of) the definition of `gcd`:

$$\gcd(n,m) = \begin{cases} n & \text{if } n \mid m \\ \gcd(\text{rem}(n,m), m) & \text{otherwise} \end{cases} \qquad (4)$$

so

$$\gcd(n,m) = \gcd(n-m,m) = \gcd(n+km,m) \qquad (5)$$

▸ Proof

RTP: $\text{CD}(n+km,m) = \text{CD}(n,m)$.
RTP: $\forall\, d \in \mathbb{Z}^+.\, (d \in \text{CD}(n+km,m) \iff d \in \text{CD}(n,m))$.
i.e. $\forall\, d \in \mathbb{Z}^+.\, (d \mid n+km) \land d \mid m \iff d \mid n \land d \mid m$.
Let $d \in \mathbb{Z}^+$.
RTP: $(d \mid n+km) \land d \mid m \iff d \mid n \land d \mid m$.
Assume $d \mid m$ (i.e. $m = ld$). (i)
RTP: $d \mid n+km \iff d \mid n$.
RTP: $id = n+km \iff jd = n$ for some $i, j \in \mathbb{Z}$.
Using (1), RTP: $id = n + k(ld) \iff jd = n$.
RTP: $(i - kl)d = n \iff jd = n$ which is clearly true.
Hence, $\text{CD}(n+km,m) = \text{CD}(n,m)$.
Hence, $\gcd(n+km,m) = \gcd(n,m)$.

`egcd` (Extended gcd algorithm)

Basically go down the recursive definition given in (4), but also write down at each stage an equation for each argument in terms of the original arguments:
- In the original iteration, $n = N$ and $m = M$. - In later iterations, we already have one of them, and $\text{rem}(n,m) = n - (\text{quo}(n,m))m$ and use the n and m from the previous recursion iteration.

Thus, we get

$$\gcd(n,m) = kn + lm \qquad (6)$$

Sets

Cardinality: size of set, $\# S$,

Powerset: set of all of its subsets, $\mathcal{P}(U)$

- $x \in \mathcal{P}(U) \iff x \subseteq U$
- $\emptyset \in \mathcal{P}(U)$
- $U \in \mathcal{P}(U)$
- $\#\mathcal{P}(U) = 2^{\# U}$

Family: some set containing subsets of U, $\mathcal{F} \subseteq \mathcal{P}(U)$ (so $\mathcal{F} \in \mathcal{P}(\mathcal{P}(U))$).

Product of 2 sets: $A \times B = \{(a,b) \mid x \in A, b \in B\}$.