Number theory exercises WS 2019, TU Graz

Sheet 1, solutions (on paper) to be handed in on 8th October 2019

1-1. a) Why is the following proof wrong? There are infinitely many primes. Suppose there are finitely many primes $p_1, \dots, p_k$ only, then $1 + \prod_{i=1}^k p_i$ is a new prime.

b) Work through the **second proof** of Euclid's theorem on primes from chapter 1 of "Proofs from the book". The German version is freely available if you are logged into a Tu account (e.g. with vpn). https://link.springer.com/book/10.1007/978-3-662-57767-7
An old English version (old edition) is also freely available at
https://www.emis.de/classics/Erdos/textpdf/aigzieg/aigzieg.pdf

1-2. Work through the sixth proof of Euclid's theorem on primes from chapter 1 of "Proofs from the book".

1-3. Find an increasing squence (s_i) of (infinitely many) positive integers, such that $\gcd(s_i, s_j) = 1$ for all $i \neq j$, and conclude that there are infinitely many primes. (The sequence should not be the sequence of Fermat numbers F_n.)

1-4. Work through a proof of Schur's theorem, and look up a version of Ramsey's theorem (no proof required) to make sure you understand the proof.

Schur's theorem [2], **(1916)**
For every positive integer t there exists an integer s_t, such that if one colours each integer $m \in [1, s_t]$ by one of t distinct colours, then there is a monochromatic solution of $a + b = c, a, b, c \in [1, s_t]$.

Proof: We show that Schur's theorem can be seen as a direct consequence of Ramsey's theorem (1930). Ramsey's theorem (see [1], Theorem 10.3.1) states that for any number t of colours (let us call them $1, \dots, t$) and positive integers $n_1, \dots, n_t$ there exists an integer $R(n_1, \dots, n_t)$ such that if the edges of the complete graph on $R(n_1, \dots, n_t)$ vertices are coloured there exists an index i and a monochromatic clique of size n_i all of whose edges are of colour i. In our application we only need the case $n_1 = \dots = n_t = 3$.

Let $\chi : \{1, \dots, N\} \to \{1, \dots, t\}$ be the colouring of the first $N = R(n_1, \dots, n_t)$ integers. Let us define a colouring of the *edges* of the complete graph with vertices $\{1, 2, \dots, N\}$ as follows: The edge (i, j) is given the colour $\chi(|i-j|)$. Ramsey's theorem guarantees that there is a monochromatic triangle. Let us denote the vertices of this triangle by (i, j, k), where $i < j < k$. Let $a = j - i, b = k - j$ and $c = k - i$. Then a, b, c all have the same colour and $a + b = c$ holds. This gives the requested monochromatic solution.

1-5. Give full details of the following sketch of a proof. Suppose there are finitely many primes only, $p_1, \dots, p_k$, then show that the number of ways to write intgers $n \leq N$ as $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is only about $(\log N)^k$ and conclude that this is much smaller than N.

Apply this argument to the sequence $\{a^2 + 1 : a \in \mathbb{N}\}$ and conclude there are infinitely many primes which are divisors of some number of the form $a^2 + 1$. Prove that odd prime divisors of $a^2 + 1$ are always 1 mod 4. Conclude there are infinitely many primes of the form $p \equiv 1 \bmod 4$.

1-6. For $n \geq 3$, call a positive integer n-smooth if none of its prime factors is larger than n. Let S_n be the set of all n-smooth positive integers. Let C be a finite, nonempty set of nonnegative integers, and let a and d be positive integers. Let M be the set of all positive integers of the form $m = \sum_{k=1}^d c_k s_k$, where $c_k \in C$ and $s_k \in S_n$ for $k = 1, \dots, d$. Prove that there are infinitely many primes p such that $p^a \notin M$.

1-7. Prove that $\sum_{n=1}^\infty \frac{1}{n^2} = \prod_p \frac{1}{1-1/p^2}$. Recall that $\sum_{n=1}^\infty \frac{1}{n^2} = \frac{\pi^2}{6}$, and that π^2 is irrational. (No proofs required for this.) Conclude that there are infinitely many primes.

Hand in solutions to 1.1a) 1.3), 1.5), 1.6) and 1.7). (((For 1.1b), 1.2), 1.4) you can hand it in, if you actually have more details or comments than the original proofs.))) For ticking the boxes (crosses) in teh onlien-kreuze-system, do all 7 problems, if you are ready to explain them on the board in class.

Deadline for crosses are: Tuesday 9.55am.

https://www.math.tugraz.at/∼elsholtz/WWW/lectures/ws19/numbertheory/vorlesung.html

References

[1] P.J. Cameron, Combinatorics: Topics, Techniques, Algorithms, Cambridge University Press, 1995.

[2] I. Schur, Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$, Jahresbericht der Deutschen Mathematischen Vereinigung 25 (1916), 114—117.