Algebra and discrete mathematics, homework sheet 3

Due: 10 March 2015, 8:45

You can hand in groups of size two or three; specify names and student numbers. To hand in send *email* to `tanja@hyperelliptic.org` with your program. Please include your program as a .txt or .sage file or save it as a worksheet.

This sheet is part of the regular homework and counts towards your grade; sorry for the confusing information on Oase.

1. Let p be a prime. Write three programs to find a generator of the multiplicative group of $\mathbb{Z}/p$ as specified below. None of them should use `Zmod(p).unit_gens()` or `Zmod(p).multiplicative_generator()`.
   (a) Use the `.multiplicative_order()` command.
   (b) Use the list of divisors of $p-1$ to check for the order. This should use the `divisors(p-1)` command.
   (c) Use that a is a generator if and only if $a^{(p-1)/p_i} \not\equiv 1 \bmod p$ for all primes $p_i | (p-1)$. This should use the `factor(p-1)` command and be significantly faster than the previous method.
2. Write a program that computes all generators of the multiplicative groug $(\mathbb{Z}/p)^\times$. Note that for p a prime this group contains all non-zero elements in $\mathbb{Z}/p$.
3. Compute the order of the multiplicative group of $\mathbb{Z}/12347$ and of $\mathbb{Z}/12345$.
4. Compute the number of generators of the multiplicative group of $\mathbb{Z}/12347$.
5. Compute all subgroups of $(\mathbb{Z}/15, +) \times (\mathbb{Z}/12, +)$.
6. Let $\mathbb{Z}/15 = \langle r \rangle$ and $\mathbb{Z}/12 = \langle s \rangle$. Compute the subgroup generated by (r^2, s^4) and (r^3, s^2)