UNIVERSITY OF ST ANDREWS

Finite Mathematics Problem Set 1

Igor Rivin

December 2, 2015

1 EXERCISE 1

Use the Extended Euclidean Algorithm to compute the greatest common divisors (and the linear combinations of the arguments leading to the common divisors of

- 17 and 23
- 2^{17} and 3^{23}
- $20! + 1$ and $17! + 2$.

Solution:

-

$$
\begin{aligned}
23 &= 17 \times 1 + 6 \\
17 &= 6 \times 2 + 5 \\
6 &= 5 \times 1 + 1
\end{aligned}
$$

So, $1 = 6 - 5 = (23 - 17) - (17 - 6 \times 2) = (23 - 17) - (17 - (23 - 17) \times 2) = 23 \times 3 - 17 \times 4.$

- $$\begin{aligned} 3^23 &= 94143178827 \\ 2^17 &= 131072 \\ 3^23 &= 2^17 \times 718255 + 59467 \\ 2^17 &= 59467 \times 2 + 12138 \\ 58467 &= 12138 \times 4 + 10915 \\ 12138 &= 10915 \times 1 + 1223 \\ 10915 &= 1223 \times 8 + 1131 \\ 1223 &= 1131 \times 1 + 92 \\ 1131 &= 92 \times 12 + 27 \\ 92 &= 27 \times 3 + 11 \\ 27 &= 11 \times 2 + 5 \\ 11 &= 5 \times 2 + 1 \end{aligned}$$

  Combining as before, get

  $$1 = -3^{23} \times 24221 + 2^{17} \times 17396865344.$$

- As before, get

  $$1 = -8580806438459 \times (20! + 1) + 58692716039059230 \times (17! + 2).$$

2 EXERCISE 2

Compute $17^{129} \mod 361$,
Solution:

$$\begin{aligned} 17^2 = 289 \equiv -72 &\mod 361. \\ 17^4 \equiv 72^2 \equiv 130 &\mod 361. \\ 17^8 \equiv 130^2 \equiv 294 &\mod 361 \\ 17^{16} \equiv 157 &\mod 361 \\ 17^{32} \equiv 101 &\mod 361 \\ 17^{64} \equiv 93 &\mod 361 \\ 17^{128} \equiv 346 \equiv -15 &\mod 361 \\ 17^{129} = 17^{128} \times 17 \equiv 255 &\mod 361. \end{aligned}$$

3 Exercise 3

Compute the smallest positive number x, such that $17x \equiv 1 \mod 65537$. Solution:

$$1 = 17 \times 30841 - 8 \times 65537,$$

so $x = 30841$.

4 Exercise 4

- find all the subgroups of the *additive* group of $\mathbb{Z}/17\mathbb{Z}$.
- find all the subgroups of the *multiplicative* group of $\mathbb{Z}/17\mathbb{Z}$.
- In both cases, find all the cosets of the subgroups you find.

Solution: The additive group is a cyclic group of order 17, which is prime. This means that there are only two subgroups: the subgroup $\{1\}$, and the whole group. Each element corresponds to a coset of the identity (so there are 17 of them) and the only coset of the whole group is the group itself.
The multiplicative group is a cyclic group of order 16, so its subgroups are of order $1, 2, 4, 8, 16$. since the equation $x^k - 1$ has only k solutions mod 17, there is only one subgroup of each of these orders, and the cosets of the subgroup of order two correspond to equivalence classes mod 8, of order 4 to equivalence classes mod 4, order eight to equivalence classes mod 2.