UNIVERSITY OF ST ANDREWS

Finite Mathematics Problem Set 2

Igor Rivin

December 2, 2015

1 EXERCISE 1

Prove that

$$(p-1)!+1 \equiv 0 \mod p$$

Solution: The equation $x^2-1 \equiv 0 \mod p$ has exactly two solutions: ± 1. Every other element is different from its inverse, and so cancels it in the factorial, leaving -1 as the value.

2 EXERCISE 2

Let $\mathscr{F}$ be a field of characteristic p. Prove that for any $a, b \in \mathscr{F}$,

$$(a+b)^p = a^p + b^p$$

Solution: By the binomial theorem,

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$

Every binomial coefficient in the sum is divisible by p, hence zero in a field of characteristic p.

3 EXERCISE 3

How does the previous exercise not contradict the fact that an polynomial of degree p has at most p roots over a field?
Solution: The two sides of the equation above are formally equal in a field of characteristic p, so the fact does not apply.

4 EXERCISE 4

- Compute $\phi(1728)$.
- Prove that $\sum_{d|n} \phi(d) = n$ by using the multiplicativity of ϕ.

Solution:

- $$\phi(1728) = \phi(12^3) = \phi(2^6 2^3) = \phi(2^6)\phi(3^3) = 32 \times 18 = 576$$
- First check that if f is a multiplicative function, then so is $G(n) = \sum_{d|n} f(d)$. Then check the result for prime powers.