Cryptography
(Math 4613)
Challenge IV
Wilson's Theorem
Paul L. Bailey
October 17, 2007

This sequence of problems, together with information from the notes *Cryptography Topic II: Integers*, *Cryptography Topic III: Modular Arithmetic*, and especially *Cryptography Topic VI: Algebraic Categories*, leads to a proof of Wilson's Theorem.

This challenge is complete when the ultimate winner presents the proof of Wilson's Theorem to the class. However, proofs of the individual parts will also receive points, when presented in class. You may use the statements of previous problems in your proof of a given problem, even if you haven't solved the previous problem yet.

Recall that if G is a group and $g \in G$ with $\text{ord}(g) = n$, then

$$g^m = 1 \Leftrightarrow n \mid m.$$

To show that two positive integers are equal, it suffices to show that each divides the other.

Problem 1. Let G be a group and let $g \in G$. Let $n = \text{ord}(g)$, where $n \in \mathbb{Z}$. Let $k \in \mathbb{Z}$.

(a) Let $d = \gcd(k, n)$. Show that $\text{ord}(g^d) = \text{ord}(g^k)$ (hint: use $kx + ny = d$).

(b) Show that $\text{ord}(g^d) = \frac{n}{d}$.

(c) Conclude that $\text{ord}(g^k) = \frac{n}{d}$.

Problem 2. Let G be a cyclic group of even order. Show that G contains exactly one element of order two.

Problem 3. Let G be a group with $a, b \in G$. Let $\text{ord}(a) = m$ and $\text{ord}(b) = n$, where $m, n \in \mathbb{Z}$. Suppose that $ab = ba$ and $\gcd(m, n) = 1$. Show that $\text{ord}(ab) = mn$.

Problem 4. Let G be a finite abelian group, and let n be a positive integer. Let

$$T_n(G) = \{g \in G \mid g^n = 1\}.$$

(a) Show that if $a, b \in T_n(G)$, then $ab \in T_n(G)$.

(b) Conclude that that $T_n(G) \leq G$.

Problem 5. Let F be a field and let G be a finite subgroup of F^*. Let p be a positive prime integer which divides $|G|$, and let p^r be the highest power of p which divides $|G|$. Show that $T_{p^r}(G)$ is cyclic (hint: use the fact that the polynomial $f(x) = x^{p^r} - 1$ has at most p^r roots in F).

Problem 6. Let F be a finite field. Show that F^* is cyclic.

Problem 7 (Wilson's Theorem)**.** Let p be a positive prime integer. Show that

$$(p-1)! \equiv -1 \pmod{p}.$$