1 Elementary number theory, III

The setup is the same as in Worksheets I and II. You may assume all the Propositions from Worksheet I and from Worksheet II.

Proposition 22. *For any integers a, b, c and d and any natural number n, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $a + c \equiv b + d \bmod n$.*

Proposition 23. *For any integers a, b, c and d and any natural number n, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $ac \equiv bd \bmod n$.*

Proposition 24. *For any integers a, b, c and d and any natural number n, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $a - c \equiv b - d \bmod n$.*

Proposition 25. *For any integers a and b and any natural number n, if $a \equiv b \bmod n$ then $a^2 \equiv b^2 \bmod n$.*

Conjecture 26. *For any integers a and b and any natural number n, if $a \equiv b \bmod n$ then for all positive integers k, we have $a^k \equiv b^k \bmod n$.*

Definition 27. *Let S be a set of integers. We say an element l in S is a* least element *(or a* smallest element*) of S if for every s in S we have $l \leq s$.*

Remark 28. *We will assume that the following statement about the natural numbers is true:*

If S is any non-empty set of natural numbers then S has a least element.

We'll refer to this statement as the 'Well-ordering Principle'.

Theorem 29. *Let a be an integer and let b be a natural number. Then there exist integers q and r such that $a = bq + r$ and $0 \leq r < b$.*

For the proof of Theorem 31 below, you may find the following lemma useful. [Prove it first.]

Lemma 30. *Let a and b be integers and let c be a natural number. If $0 \leq a < c$ and $0 \leq b < c$ then $-c < a - b < c$, or equivalently $|a - b| < c$.*

Theorem 31. *Let a be an integer and let b be a natural number. If there exists integers q, q', r and r' such that $a = bq + r$, $0 \leq r < b$ and $a = bq' + r'$, $0 \leq r' < b$ then $q = q'$ and $r = r'$.*