This document contains a list of results that are granted without proof, or that were proven and accepted by the class. You may cite the granted results by number, e.g. "by G.1" . If a result does not appear on one of these lists and we have not proved it, then the Rules of the Game still apply.

As we proceed through the problem/theorem sequence in the textbook, you may wonder which results you are allowed to use. In general, you may use the basic algebra and ordering of the integers, the Well-Ordering Principle, standard logic and proof techniques such as cases, contradiction, contraposition, and induction, any result we have proven earlier in the sequence, and anything I have explicitly granted us. When in doubt: *prove it before you use it.* When using a previous result from the textbook you should cite it by number.

Granted Results

You may freely use the following results without proof.

G.1 Cancellation in $\mathbb{Z}$. Let $a, b, c \in \mathbb{Z}$ with $c \neq 0$. If $ac = bc$, then $a = b$.

The proof is a short argument relying on the order properties of $\mathbb{Z}$, which we are taking as given. Note: in class, several counterexamples were provided to the corresponding statement modulo n (see Question 1.20).

Results Established in Class

Numbered items refer to *Number Theory Through Inquiry*; items beginning with R refer to Supplement R. All of the following are available for you to cite.

1.1 Divisibility is preserved by sums.

1.2 Divisibility is preserved by differences.

1.3 Divisibility of a product, from divisibility of both factors.

1.4 The hypothesis $a \mid c$ in 1.3 is unnecessary, and the conclusion can be strengthened to $a^2 \mid bc$.

1.5 Conjectures raised and settled in class.

1.6 Divisibility is preserved by multiples.

1.7 Small divisibility and congruence computations.

1.8 Characterizations of the integers in several congruence classes.

1.9 Congruence modulo n is reflexive.

1.10 Congruence modulo n is symmetric.

1.11 Congruence modulo n is transitive.

R.9 Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

1.12 Congruence classes may be added.

1.13 Congruence classes may be subtracted.

1.14 Congruence classes may be multiplied.

1.20 Cancellation property *fails* modulo n in general.

R.13 Basic properties of equivalence classes.

Open Questions

Questions raised in class that have not been proved.

- Which integers *can* be "canceled" modulo n?