Math 104a: Number theory – List of results covered in class or in section

François Thilmany

Thursday 19 July 2018

Below is a non-exhaustive list of results that were covered in class, section or homework. You can use these results without reproving them, provided it is not the point of the question and you make a clear reference either to the name of the theorem or by recalling the statement. If in doubt, ask!

From the homework, unless it is part of the question, you may quote by recalling the statement:

HW1: problems 1, 3, 9, 12, and 13.
HW2: problems 4, 5, 7, 8, and 10.
HW3: problems 7, 8, 11, and 13.
HW4: problems 1, 2, 3, 12, and 13.
HW5: problems 1, 2, 3, 6, 7, 8, 12, and 13.

From lectures, you may quote the following results.

Theorem (Euclidean division in $\mathbb{Z}$)**.** *Let $a \in \mathbb{Z}$ and $b \in \mathbb{N} - \{0\}$. There exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

Theorem (Bézout's identity in $\mathbb{Z}$)**.** *Any two integers a, b have a greatest common divisor (gcd). If d is a gcd of a and b, there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$.*

Lemma (Euclid's lemma in $\mathbb{Z}$)**.** *If $p \in \mathbb{Z}$ is irreducible, then p is prime.*

Theorem (Unique factorization in $\mathbb{Z}$)**.** *Every nonzero $a \in \mathbb{Z}$ can be written as*

$$a = \pm p_1^{e_1} \dots p_r^{e_r}$$

where the p_i's are distinct positive primes and $e_i \in \mathbb{N} - \{0\}$ (possibly $r = 0$, in which case the empty product is understood to be 1). Moreover, this factorization is unique up to rearranging the primes p_i.

Proposition (Computing gcd's using the Euclidean algorithm)**.** *Let $a, b \in \mathbb{N}$ and assume $a \geq b$. Then $\gcd(a, b)$ is the last non-zero term in the sequence (r_k) constructed inductively as follows:*

$r_{-1} = a$, $r_0 = b$, and given r_{k-1} and $r_k \neq 0$, define r_{k+1} to be the remainder of the Euclidean division of r_{k-1} by r_k:

$$r_{k-1} = r_k q + r_{k+1} \qquad 0 \leq r_{k+1} < r_k.$$

Theorem (Infinitude of primes in $\mathbb{Z}$)**.** *There are infinitely many (positive) prime numbers in $\mathbb{Z}$.*

Theorem (Solution of linear diophantine equations)**.** *Let $a, b, c \in \mathbb{Z}$. The linear diophantine equation*

$$ax + by = c$$

has a solution $(x_0, y_0) \in \mathbb{Z}^2$ if and only if $d := \gcd(a, b)$ divides c. If so, any solution is of the form $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ for some $t \in \mathbb{Z}$.

Proposition (Prime elements are irreducible)**.** *Let R be a ring and $p \in R$ a prime. Then p is irreducible in R.*

Theorem (Bézout's identity in Euclidean domains)**.** *Any two elements a, b of a Euclidean domain D have a gcd. If $d \in D$ is a gcd of a and b, there exist $x, y \in D$ such that $ax + by = d$.*

Lemma (Euclid's lemma in Euclidean domains)**.** *Let D be a Euclidean domain. If $p \in D$ is irreducible, then p is prime.*

Theorem (Unique factorization in Euclidean domains)**.** *Let D be a Euclidean domain. Any $a \in D - \{0\}$ can be written as*

$$a = up_1^{e_1} \dots p_r^{e_r}$$

where u is a unit, the p_i's are pairwise non-associate primes in D and $e_i \in \mathbb{N} - \{0\}$. (Possibly $r = 0$, in which case the right hand side is just u.) Moreover, this factorization is unique up to rearranging the primes p_i and multiplying u or the p_i's by units.

Proposition. *The set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a Euclidean domain when endowed with addition and multiplication of complex numbers and with the Euclidean function*

$$N : \mathbb{Z}[i] \to \mathbb{N} : a + bi \mapsto a^2 + b^2.$$

Moreover, the function N is (strongly) multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{Z}[i]$.

Theorem (Classification of Pythagorean triples)**.** *The set T of primitive Pythagorean triples $(a, b, c) \in \mathbb{Z}^3$ with $a, b, c > 0$ and a odd is parametrized by*

$$T = \left\{(m^2 - n^2, 2mn, m^2 + n^2) \mid m, n \in \mathbb{Z}, m > n > 0, \gcd(m, n) = 1 \text{ and } m, n \text{ have different parity}\right\}.$$

Proposition (Construction of ring quotients)**.** *Let I be an ideal of a ring R. There exists a unique ring structure on the set $R/I := \{a+I \mid a \in R\}$ of equivalence classes modulo I for which the map*

$$R \to R/I : a \mapsto a+I$$

is a ring homomorphism.

Theorem (Isomorphism theorem for rings)**.** *Let $\varphi : R \to S$ be a homomorphism of rings. Then $\ker\varphi := \{x \in R \mid \varphi(x) = 0\}$ is an ideal of R, $\operatorname{im}\varphi := \{\varphi(x) \mid x \in R\}$ is a (sub)ring (of S), and φ induces an isomorphism*

$$\overline{\varphi} : R/\ker\varphi \to \operatorname{im}\varphi : x + \ker\varphi \mapsto \varphi(x).$$

Proposition. *Let I be an ideal of a ring R.*

(i) I is prime if and only if R/I is an integral domain.

(ii) I is maximal if and only if R/I is a field.

Theorem. *Let $m \in \mathbb{N}$ and assume $m \neq 0, 1$. An element $a + m\mathbb{Z} \in \mathbb{Z}_m$ has a multiplicative inverse in $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$. In consequence, $\mathbb{Z}_m$ is a field iff $\mathbb{Z}_m$ is a domain iff m is a prime number.*

Theorem (Chinese remainder theorem)**.** *Let $I_1, \ldots, I_n$ be pairwise comaximal ideals and set $I = I_1 \cap \cdots \cap I_n$. Then the map*

$$R/I \to R/I_1 \times \cdots \times R/I_n : x + I \mapsto (x + I_1, \ldots, x + I_n)$$

is an isomorphism of rings.

Theorem (Chinese remainder theorem for $\mathbb{Z}$)**.** *Let $m \in \mathbb{N} - \{0, 1\}$ and write $m = p_1^{e_1} \ldots p_r^{e_r}$ for some distinct, positive primes p_i. Then*

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}.$$

Corollary (Solving systems of congruences)**.** *Let $m \in \mathbb{N} - \{0, 1\}$ and write $m = p_1^{e_1} \ldots p_r^{e_r}$ for some distinct, positive primes p_i. Let $a, b \in \mathbb{Z}$. Then the congruence $ax \equiv b \mod m$ is equivalent to the system of congruences*

$$\begin{cases} ax \equiv b \mod p_1^{e_1} \\ ax \equiv b \mod p_2^{e_2} \\ \quad\vdots \qquad\qquad \vdots \\ ax \equiv b \mod p_r^{e_r}. \end{cases}$$

In consequence, any system of congruences

$$\begin{cases} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \\ \quad \vdots \qquad\quad \vdots \\ a_l x \equiv b_l \mod m_l. \end{cases}$$

can be replaced by an equivalent system of congruences with prime-power moduli, and in turn, if the latter is consistent, by a single congruence with modulus $\operatorname{lcm}(m_1, \dots, m_r)$.

Proposition. *The congruence* $ax \equiv b \mod m$ *has a solution* $x \in \mathbb{Z}$ *iff* $d = \gcd(a, m)$ *divides* b. *If so, all solutions* $x \in \mathbb{Z}$ *are solution of the congruence* $\frac{a}{d}x \equiv \frac{d}{b} \mod \frac{m}{d}$ *and vice-versa.*

Proposition (φ is weakly multiplicative)**.** *The Euler totient function* φ *is weakly multiplicative, that is, if* $\gcd(m, n) = 1$ *, then* $\varphi(mn) = \varphi(m)\varphi(n)$. *In particular, if* $m = p_1^{e_1} \dots p_r^{e_r}$ *for some distinct, positive primes* p_i, *then* $\varphi(m) = \varphi(p_1^{e_1}) \dots \varphi(p_r^{e_r})$.

Proposition (φ for prime powers)**.** *Let* $p \in \mathbb{N}$ *be a prime number. Then*

$$\varphi(p^e) = p^{e-1}(p-1) = p^e(1 - \frac{1}{p}).$$

Corollary (Euler's formula)**.** *Let* $m \in \mathbb{N} - \{0, 1\}$. *Then*

$$\varphi(m) = m \cdot \prod_{\substack{p \text{ positive prime} \\ p \text{ divides } m}} \left(1 - \frac{1}{p}\right).$$

Theorem (Lagrange)**.** *Let* H *be a subgroup of a finite group* G. *Then* $\#H$ *divides* $\#G$. *In consequence, if* $g \in G$ *has order* n, *then* $\langle g \rangle := \{\dots, g^{-1}, g^0, g, g^2, \dots\}$ *is a subgroup of size* n, *and thus* n *divides* $\#G$.

Corollary (Euler)**.** *If* $\gcd(a, m) = 1$, *then*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

In other words, the multiplicative order of a *modulo* m *divides* $\varphi(m)$.

Corollary (Fermat's little theorem)**.** *If* $p > 0$ *is a prime number and* $a \in \mathbb{Z}$ *is not divisible by* p, *then*

$$a^{p-1} \equiv 1 \mod p.$$

In consequence, for any $a \in \mathbb{Z}$, $a^p \equiv a \mod p$.

Theorem. *Let* F *be a field and* $P \in F[x] - \{0\}$ *a non-zero polynomial of degree* n *with coefficients in* F. *Then* P *has at most* n *distinct roots in* F.

Theorem (Wilson). *$p \in \mathbb{N} - \{0\}$ is prime if and only if $(p-1)! \equiv -1 \mod p$.*

Proposition (Order of elements in cyclic groups and counting them by order). *Let C be a cyclic group of size n generated by some element $g \in C$ and let $k \in \mathbb{Z}$. Then the order of g^k is $\frac{n}{\gcd(k,n)}$. In consequence, the number of elements of order $d \in \mathbb{N}$ in C is either $\varphi(d)$ if d divides n, or 0 otherwise.*

Corollary.

$$n = \sum_{\substack{d \text{ divides } n \\ 0<d\leq n}} \varphi(d)$$

Theorem (Finite subgroups of multiplicative groups of fields are cyclic). *Let F be a field and G be a finite subgroup of $F^\times$ $(= F - \{0\})$. Then G is a cyclic group.*

Corollary (Multiplicative groups of finite fields are cyclic). *If F is a finite field, then $F^\times$ is cyclic. In particular, $\mathbb{Z}_p^\times$ is cyclic when $p > 0$ is a prime number.*

Theorem (Order of elements in $\mathbb{Z}_{p^n}^\times$). *Let $p > 0$ be a prime number and $a \in \mathbb{Z}$ such that p does not divide a. Let t be the order of $a + p\mathbb{Z}$ in $\mathbb{Z}_p^\times$ and let p^m be the largest power of p which divides $a^t - 1$. Then, provided either $m > 1$ or $p > 2$, the order t_n of $a + p^n\mathbb{Z}$ in $\mathbb{Z}_{p^n}^\times$ is*

$$t_n = \begin{cases} t & \text{if } n \leq m \\ tp^{n-m} & \text{if } n \geq m. \end{cases}$$

Corollary. *If $p > 2$ is a prime number and $n \in \mathbb{N} - \{0\}$, then $\mathbb{Z}_{p^n}^\times$ is a cyclic group (of size $\varphi(p^n) = p^{n-1}(p-1)$).*

Proposition. *$\mathbb{Z}_{2^n}^\times$ is cyclic (of size 1 or 2) if and only if $n = 1$ or 2. Otherwise, if $n \geq 3$ then $\mathbb{Z}_{2^n}^\times$ is isomorphic to $C_2 \times C_{2^{n-2}}$.*

Theorem (Structure of $\mathbb{Z}_m^\times$). *Let $m \in \mathbb{N} - \{0, 1\}$ and write $m = 2^e p_1^{e_1} \dots p_r^{e_r}$ for some positive, distinct primes $p_i > 2$. If $e \leq 2$, then*

$$\mathbb{Z}_m^\times \cong C_{\varphi(2^e)} \times C_{\varphi(p_1^{e_1})} \times \cdots \times C_{\varphi(p_r^{e_r})}.$$

If $e \geq 3$, then

$$\mathbb{Z}_m^\times \cong \left(C_2 \times C_{\frac{1}{2}\varphi(2^e)}\right) \times C_{\varphi(p_1^{e_1})} \times \cdots \times C_{\varphi(p_r^{e_r})}.$$

Corollary (When is $\mathbb{Z}_m^\times$ cyclic?). *Let $m \in \mathbb{N} - \{0, 1\}$. $\mathbb{Z}_m^\times$ is a cyclic group if and only if m is of the form $2, 4, p^n$ or $2p^n$ for some prime $p > 2$ and $n \in \mathbb{N} - \{0\}$.*

Theorem (Euler's criterion). *Let $p > 0$ be an odd prime. $a \in \mathbb{Z}_p^\times$ is a square if and only if*

$$a^{\frac{p-1}{2}} = 1.$$

Equivalently, a is not a square if and only if $a^{\frac{p-1}{2}} = -1$.

Proposition (Properties of the Legendre symbol)**.** *Let $p > 0$ be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)$ has the following properties:*

(i) $\left(\frac{a}{p}\right)$ *only depends on* $a + p\mathbb{Z}$*.*

(ii) $\left(\frac{a^2}{p}\right) = 0$ *or* 1 *depending if* p *divides* a *or not.*

(iii) $\left(\frac{a}{p}\right)$ *is (strongly) multiplicative in the first entry, that is for any* $a, b \in \mathbb{Z}$*,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(iv) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \mod 4 \text{ or if } p = 2 \\ -1 & \text{if } p = -1 \mod 4 \end{cases}$.

Theorem (Gauss' lemma)**.** *Let $p > 0$ be an odd prime and $a \in \mathbb{Z}$ be such that p does not divide a. Let μ count the number of negative remainders obtained when reducing the elements $a, 2a, \ldots, \frac{p-1}{2}a$ modulo p to the set $\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Corollary (When is 2 is a square mod p?)**.** *Let $p > 0$ be an odd prime. 2 is a square in $\mathbb{Z}_p$ if and only if $p = \pm 1 \mod 8$. Equivalently, 2 is not a square in $\mathbb{Z}_p$ if and only if $p = \pm 3 \mod 8$.*

Theorem (Quadratic reciprocity law)**.** *Let $p, q > 0$ be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

unless p and q are both congruent to -1 modulo 4, in which case

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Equivalently,

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$