Authors of GNU MP (in chronological order of initial contribution)

Torbjörn Granlund Main author

John Amanatides Original version of mpz/pprime\_p.c

Paul Zimmermann mpn/generic/mul\_fft.c, now defunct dc\_divrem\_n.c,

rootrem.c, old mpz/powm.c, old toom3 code.

Ken Weber Now defunct mpn/generic/bdivmod.c, old mpn/generic/gcd.c

Bennet Yee Previous versions of mpz/jacobi.c mpz/legendre.c

Andreas Schwab mpn/m68k/lshift.asm, mpn/m68k/rshift.asm

Robert Harley Old mpn/generic/mul\_n.c, previous versions of files in

mpn/arm

Linus Nordberg Random number framework, original autoconfery

Kent Boortz MacOS 9 port, now defunct.

Kevin Ryde Most x86 assembly, new autoconfery, and countless other

things (please see the GMP manual for complete list)

Gerardo Ballabio gmpxx.h and C++ istream input

Pedro Gimeno Mersenne Twister random generator, other random number

revisions

Jason Moxham Previous versions of mpz/fac\_ui.c and gen-fac\_ui.c

Niels Möller gen-jacobitab.c,

mpn/generic/hgcd2.c, hgcd.c, hgcd\_step.c,

hgcd\_appr.c, hgcd\_matrix.c, hgcd\_reduce.c,

gcd.c, gcd\_11.c, gcd\_22.c, gcdext.c, matrix22\_mul.c,

gcdext\_1.c, gcd\_subdiv\_step.c, gcd\_lehmer.c,

gcdext\_subdiv\_step.c, gcdext\_lehmer.c,

jacobi\_2.c, jacbase.c, hgcd\_jacobi.c, hgcd2\_jacobi.c,

matrix22\_mul1\_inverse\_vector.c,

toom\_interpolate\_7pts, mulmod\_bnm1.c, dcpi1\_bdiv\_qr.c,

dcpi1\_bdiv\_q.c, sbpi1\_bdiv\_qr.c, sbpi1\_bdiv\_q.c,

sec\_invert.c,

toom\_eval\_dgr3\_pm1.c, toom\_eval\_dgr3\_pm2.c,

toom\_eval\_pm1.c, toom\_eval\_pm2.c, toom\_eval\_pm2exp.c,

divexact.c, mod\_1\_1.c, div\_qr\_2.c,

div\_qr\_2n\_pi1.c, div\_qr\_2u\_pi1.c, broot.c,

brootinv.c,

mpn/x86/k7/invert\_limb.asm, mod\_1\_1.asm,

mpn/x86\_64/invert\_limb.asm,

invert\_limb\_table.asm, mod\_1\_1.asm,

div\_qr\_2n\_pi1.asm, div\_qr\_2u\_pi1.asm,

mpn/x86\_64/core2/aorsmul\_1.asm,

mpz/nextprime.c, divexact.c, gcd.c, gcdext.c,

jacobi.c, combit.c, mini-gmp/mini-gmp.c.

Marco Bodrato mpn/generic/toom44\_mul.c, toom4\_sqr.c, toom53\_mul.c,

toom62\_mul.c, toom43\_mul.c, toom52\_mul.c, toom54\_mul.c,

toom\_interpolate\_6pts.c, toom\_couple\_handling.c,

toom63\_mul.c, toom\_interpolate\_8pts.c,

toom6h\_mul.c, toom6\_sqr.c, toom\_interpolate\_12pts.c,

toom8h\_mul.c, toom8\_sqr.c, toom\_interpolate\_16pts.c,

mulmod\_bnm1.c, sqrmod\_bnm1.c, nussbaumer\_mul.c,

toom\_eval\_pm2.c, toom\_eval\_pm2rexp.c,

fib2m.c, strongfibo.c,

mullo\_n.c, sqrlo.c, invert.c, invertappr.c;

mpn/x86/atom/aors\_n.asm, aorslshC\_n.asm,

aorrlsh{1,2,C}\_n.asm, aorsmul\_1.asm, logops\_n.asm,

sublsh2\_n.asm, rshift.asm; primesieve.c;

mpz/fac\_ui.c, 2fac\_ui.c, mfac\_uiui.c, oddfac\_1.c,

primorial\_ui.c, prodlimbs.c, bin\_ui.c,

lucmod.c, stronglucas.c,

goetgheluck\_bin\_uiui.c; mini-gmp/mini-mpq.c.

David Harvey mpn/generic/add\_err1\_n.c, add\_err2\_n.c,

add\_err3\_n.c, sub\_err1\_n.c, sub\_err2\_n.c,

sub\_err3\_n.c, mulmid\_basecase.c, mulmid\_n.c,

toom42\_mulmid.c,

mpn/x86\_64/mul\_basecase.asm, aors\_err1\_n.asm,

aors\_err2\_n.asm, aors\_err3\_n.asm,

mulmid\_basecase.asm,

mpn/x86\_64/core2/aors\_err1\_n.asm.

Martin Boij mpn/generic/perfpow.c

Marc Glisse gmpxx.h improvements

David Miller mpn/sparc32/ultrasparct1/{addmul\_1,mul\_1,submul\_1}.asm

mpn/sparc64/ultrasparct3/{mul\_1,addmul\_1,submul\_1}.asm

mpn/sparc64/ultrasparct3/{add\_n,sub\_n}.asm

mpn/sparc64/ultrasparct3/{popcount,hamdist}.asm

mpn/sparc64/ultrasparct3/cnd\_aors\_n.asm

mpn/sparc64/{rshift,lshift,lshiftc}.asm

mpn/sparc64/tabselect.asm

Mark Sofroniou mpn/generic/mul\_fft.c type cleanup.

Ulrich Weigand Changes to support powerpc64le:

configure.ac, mpn/powerpc64/{elf,aix,darwin}.m4,

mpn/powerpc32/{darwin,elf}.m4,

mpn/powerpc64/mode64/{dive\_1,divrem\_1,divrem\_2}.asm,

mpn/powerpc64/mode64/{gcd\_1,invert\_limb,mode1o}.asm,

mpn/powerpc64/mode64/{mod\_1\_1,mod\_1\_4}.asm,

mpn/powerpc64/mode64/p7/gcd\_1.asm,

mpn/powerpc64/p6/{lshift,lshiftc,rshift}.asm,

mpn/powerpc64/vmx/popcount.asm.