Ex3

```cpp
#include <iostream>
#include <cstdlib>
#include <gmpxx.h>
#include <gmp.h>
using namespace std;

unsigned long int extended(mpz_t a,mpz_t b,mpz_t& x,mpz_t& y) {
    mpz_t r, s, t;
    mpz_init(r);
    mpz_init_set_str(s, "1", 10);
    mpz_init(t);
    mpz_set_ui(x, 1);
    mpz_set_ui(y, 0);

    //gmp_printf("%Zd %Zd %Zd %Zd %Zd %Zd %Zd\n", a, b, x, y, m, n, t);
    mpz_t temp;
    mpz_init(temp);
    while(mpz_cmp_ui(b, 0) != 0){
        mpz_set(t, r);
        mpz_fdiv_q(temp, a, b);
        mpz_mul(temp, temp, r);
        mpz_sub(r, x, temp);
        mpz_set(x, t);

        mpz_set(t, s);
        mpz_fdiv_q(temp, a, b);
        mpz_mul(temp, temp, s);
        mpz_sub(s, y, temp);
        mpz_set(y, t);

        mpz_set(t, b);
        mpz_fdiv_r(b, a, b);
        mpz_set(a, t);
    }

    unsigned long int answer = mpz_get_ui(a);

    mpz_clear(r);
    mpz_clear(s);
    mpz_clear(t);
    mpz_clear(temp);
    return answer;
}

int main() {
    mpz_t a, b, c;
    string s1 = "", s2 = "";

    srand(time(0));
    for(int i = 0; i < 4096; i++) {
        if(rand() % 2 == 1){
            s1 += "1";
```

```
53              }
54              else s1 += "0";
55          }
56          const char *s11 = s1.c_str();
57          srand(rand() % 10);
58          for(int i = 0; i < 4096; i++) {
59              if(rand() % 2 == 0){
60                  s2 += "0";
61              }
62              else s2 += "1";
63          }
64
65          const char* s22 = s2.c_str();
66          mpz_init_set_str(a, s11, 2);
67          mpz_init_set_str(b, s22, 2);
68          mpz_init(c);
69
70          gmp_printf("%Zd\n", a);
71          gmp_printf("%Zd\n", b);
72          mpz_gcd(c, a, b);    # use the gcd function in GMP to calculate
73          gmp_printf("%Zd\n", c);
74
75          mpz_t x, y;
76          mpz_init(x);
77          mpz_init(y);
78
79          # use the Extended Euclidean Algorithm to calculate gcd
80          unsigned long int gcd = extended(a, b, x, y);
81
82          mpz_clear(a);
83          mpz_clear(b);
84          mpz_clear(c);
85          mpz_clear(x);
86          mpz_clear(y);
87          cout << gcd << endl;
88          //std::cout << s11 << endl;
89          //cout << s22 << std::endl;
90          return 0;
91      }
92
```

Above is the code for the realization of the Extended Euclidean Algorithm and the comparison between it and the gcd function inside the GMP library. The comparison is shown in the pictures below.

```
The first number:
392845262937047083353428506678705740589945306977458044697286482644908696705795320875159365488129033322053310774359276014864885681232294455100666066229778056340587565117431992249808091960563951411150055265456094492331305643975206704104230434287547975501811226390028504574361213705745102876419469270289000431453373359454127989268338439244781823343564267534969691958665295497931491863292036920877225485428650680726948362428726909924675800662379481799068371373144596115951029119632889492341068225063560619026150615252766267722419505831719719172679637800239246637451807869828981955157243077844099649338607031425027588336534313928828017989863661897609787141591932954648908189596661550150627552000377626797156335555449401034350856557378984701242661198448942718206596854711624258078231860203709211082898120244727518141636771753981455710780519553870379081647421060945794085176509717993002511728029313262366919447258139517900881137836085322656113411243306179235465771899807027165301328439139031950153918924775751514032073977391636080616442763729525512301342890166917014545842858289050198023876313918487464967514150269332822297061224239174985422063511221407453963183721727778481525969161007306785497738152811054848724757350924272640399271162 4
The second Number:
86992289325345525926154823420234823693006250740114747901700372146080894977610946598375754875252941403871692653209509159583363265709897449084848890510707938044422719203133085683668807418680097828112682669329893093240831504967430378073603395237889057368945390013810235510793647279668133357681190552271137058857547579920945287644257869179707565637964304070477946404503787158782534284987877118928617737346334649445788828413301654931914642135666499753933972286924920887839091242315138256230974114838128921652720092776265012217338104841203231970363645076304777342467648021399371441779439148520592950145497850033703029857807925479890769648817845201681525340006211171169112711787211776838878436423960130086222297688040441850511100451314078448809049382153095386797311453655214963562883432944396871852676552459192544677822749659122449953607705781275476527848673640535422618309733536147277609694969173079276654005402549656496448659090829892523126793427060666500766764086808033849242193008516501550872051264787535754789222524723908637068807665247422404134539969233815016114029230814447494099005115320779740838973726017340693255899223434924033211443183360448100013884325888416284397812911199367729534989449810414027883698170201341067249205795360302 7
gcd using mpz_gcd():
1
gcd using Extended Euclidean Algorithm:
1
```

```
The first number:
99884898634898767375034440316584682526968449894458706930707543537653555294765884995367042459224242517061450442131397139725895214116893012470209391533819354412008198399961056130140330504228391566122400667821505797459149208815978478851048080266759441684819784492243928467818658365415040589400290972844016025804769158506809497963786198767987965736508304738242209560726253136368681738459686504789938109892749121574588315746772129426579768312993561588852261249000575338632981898726778749395564620251786384369881212307925836007692223154519313646804375597550293281295177768273887913521487405941032639653229238840610840541676337289353402639199916891092246273378459483842785769344252936689335172768144590974749644716131555294839893110802767196384716890191416620492518316099132142079097191231225413002653459129360678785615715780186329320518454998219581878219655144422830595061862814852819430818556481453717565902281427207422662403453766719538019329263145530332437363846488080271270984586854409707150454801792527563371984710204413705338895345686973873837988517494978608157600418326992969862679421341429341309549411130065749225839507004690611528921353566932571215182740394683643590632978640454451530177953607620628211372606114227964096067387764933
The second Number:
86992289325345525926154823420234823693006250740114747901700372146080894977610946598375754875252941403871692653209509159583363265709897449084848890510707938044422719203133085683668807418680097828112682669329893093240831504967430378073603395237889057368945390013810235510793647279668133357681190552271137058857547579920945287644257869179707565637964304070477946404503787158782534284987877118928617737346334649445788828413301654931914642135666499753933972286924920887839091242315138256230974114838128921652720092776265012217338104841203231970363645076304777342467648021399371441779439148520592950145497850033703029857807925479890769648817845201681525340006211171169112711787211776838878436423960130086222297688040441850511100451314078448809049382153095386797311453655214963562883432944396871852676552459192544677822749659122449953607705781275476527848673640535422618309733536147277609694969173079276654005402549656496448659090829892523126793427060666500766764086808033849242193008516501550872051264787535754789222524723908637068807665247422404134539969233815016114029230814447494099005115320779740838973726017340693255899223434924033211443183360448100013884325888416284397812911199367729534989449810414027883698170201341067249205795360302 7
gcd using mpz_gcd():
7
gcd using Extended Euclidean Algorithm:
7
```

```
The first number:
67888246627150444717600762859278172199330702401081309387794086278623577882373079947486853321085051496212900890452997113407804472175221330162005845041024156081876810583187832073491534481722201496859270465262411926258510042287605260410411958236183623406782909426780414215966462184074902118702913439268129463122582981017455388424899878399518341443386878496663659096810554627041208772889756346228113554488324313555193325833776765736650565735116417997132183575461038712132638474198807391266336336986120354608767658208038247121816754226716405630063793983275540780691186910159661881677426486561150309910032412369726736551000995310227354278263225984847525961142671278613337925186972610032707828254800993654499936510147218544277320233635140202373167950739635713703277885913255962339940294885585370586581065256003382020183619916968074167572834477460390192701348333474603429040028326630795574771817263782076246551321093801203630134462891947440049421372110783471052760648553235892455753648559278626294589711120796902718527318572864290067896753061637197253786864780537225902732200218343221348578626965418784860140203193082056156006515615513083002811782612084489317078391512093128794324656414163951178389145014483705774457075779059406298228583
The second Number:
86992289325345525926154823420234823693006250740114747901700372146080894977610946598375754875252941403871692653209509159583363265709897449084848890510707938044422719203133085683668807418680097828112682669329893093240831504967430378073603395237889057368945390013810235510793647279668133357681190552271137058857547579920945287644257869179707565637964304070477946404503787158782534284987877118928617737346334649445788828413301654931914642135666499753933972286924920887839091242315138256230974114838128921652720092776265012217338104841203231970363645076304777342467648021399371441779439148520592950145497850033703029857807925479890769648817845201681525340006211171169112711787211776838878436423960130086222297688040441850511100451314078448809049382153095386797311453655214963562883432944396871852676552459192544677822749659122449953607705781275476527848673640535422618309733536147277609694969173079276654005402549656496448659090829892523126793427060666500766764086808033849242193008516501550872051264787535754789222524723908637068807665247422404134539969233815016114029230814447494099005115320779740838973726017340693255899223434924033211443183360448100013884325888416284397812911199367729534989449810414027883698170201341067249205795360302 3
gcd using mpz_gcd():
3
gcd using Extended Euclidean Algorithm:
3
```

It is obvious that the value is always the same, which means that the Extended Euclidean Algorithm we implement has the same effect as the gcd function the GMP library has.